The Global Trust Register 1998

Ross J. Anderson
Bruno Crispo
Jong-Hyeon Lee
Charalampos Manifavas
Václav Matyáš Jr.
Fabien A.P. Petitcolas

Publisher: Northgate Consultants Ltd., 10 Water End, Wrestlingworth,
Sandy, Bedfordshire SG19 2HA, United Kingdom
Copyright 1998 by Northgate Consultants

The Global Trust Register for 1998

Editors:

Ross J. Anderson
Bruno Crispo
Jong-Hyeon Lee
Charalampos Manifavas
Václav Matyáš Jr.
Fabien A.P. Petitcolas

ISBN: 0-9532397-0-5
1. Computer Security 2. Cryptography

All rights reserved. In no event will the publisher be liable for any consequential, incidental or indirect damages (including damages for loss of business profits, business interruption, loss of business information and the like) arising out of the use or inability to use the information in this book.

We accept no liability at all for any errors in the entries in this book. It is a fact of publishing life that typos occur, as do mistakes in compilation and bugs in software. We believe that we have taken reasonable care, but we have not had the time or other resources to take extreme precautions against errors and attacks.

The purpose of this book is not due diligence but risk reduction. We aim to help a prudent person to check the validity of public key certificates that are presented to her electronically; we do not aim to provide the only such means, still less to provide protection against the very large number of things that can go wrong with computer systems, or be utilised maliciously by an attacker.

Where it is necessary to be able to place legal reliance on a digital signature, the reader should obtain confirmation directly from the counterparty of the value or fingerprint of the public key or certificate, as well as of any contractual conditions, restrictions, jurisdiction and other conditions.

Cover illustration: Jirí Matyáš

This book contains 99 numbered pages.

Printed 1998-02-09.

Table of Contents

Foreword 1

1 Introduction 2

1.1 Global CA 2

1.2 Grounding Trust in a Paper Book 4

1.3 Scientific and Engineering Aspects 5

1.4 Politics 8

1.5 How We Chose and Checked the Keys 9

1.6 Disclaimer 11

1.7 Next Version 12

1.8 How to Buy a Copy 12

2 Certification Authorities 15

3 Secure Web Sites 29

4 EDI Keys 33

5 Computer Emergency Response Teams 34

6 Other Institutional Keys 43

7 Personal Keys 47

8 Medical Keys 96

9 Remailers 98

Foreword

The growth and commercial development of the Internet will depend on solving the big open question of trust. A significant part of this problem depends on having some way of identifying and authenticating users — essentially a robust way of answering the question '*To whom am I speaking?*

The probable solution to this problem involves public key cryptography. This technology lets each user generate two related keys: one key is kept private and used to create 'digital signatures' on messages, while the other is made public and used to verify them.

The question that now arises is how to find out which user is associated with which public key.

When public key cryptography came along in the 1970's, its inventors suggested that the names of computer users, and their public keys, should be published in a public directory — a kind of phone book. By the 1980's, the idea had shifted to certification authorities — bodies that would sign and issue electronic documents to the effect that 'the key with value X belongs to company Y'.

However people still have to get authentic copies of the public keys of the certification authorities themselves, and this is the principal problem which this book addresses.

The hope is sometimes expressed that all the world's numerous certifiers would sign each others' keys. However, as they are often competitors, this is unlikely to happen soon; and even if they did, it would be limited value as they often use incompatible certification policies and mechanisms.

Meantime, we believe that the kind of trust that an old-fashioned paper directory can provide will be a useful complement to the trust that can be placed in electronic certification mechanisms.

1 Introduction

This book is a register of the fingerprints of the world's most important public keys; it implements a top-level certification authority (CA) using paper and ink rather than in an electronic system.

Its purpose is fourfold:

1. to provide the currently missing top level in the global key certification hierarchy, thus enabling users to verify the authenticity of root certificates that they acquire online;
2. to ground the trust required for electronic commerce and other online applications in the trust that has been built up over the years in the world of print publishing, and thereby to build confidence in electronic trust mechanisms;
3. to broaden our understanding of the scientific, engineering and business issues associated with top-level certification, and in the process to discover as many bugs and other problems as possible in existing public key standards and their implementations;
4. to use the privilege of a print publisher — to print and distribute anything that is not pornographic, seditious or a breach of copyright — to forestall plans by some governments to license CAs and to impose oppressive licensing conditions, such as the escrow of private confidentiality keys.

We will now explore each of these purposes in turn.

1.1 Global CA

When Whit Diffie and Marty Hellman invented public key cryptography in 1975, their vision was that people would look up public keys in the phone book. But a paper listing of billions of people is large and including keys would make it worse, so the phone companies elaborated the idea into a standard for a distributed electronic database (X.500). Although the key certificate part of this (X.509) is becoming widely used, the central database was never built. Now it probably will not be. The business model of a single, state-owned phone company in each country has been superseded; there are now many competing phone companies, and many more firms providing Internet and other data services. People use a wide variety of mechanisms, from specialist directories to web search engines, to find other people; and the X.400 email mechanism that underlies X.500 has been defeated in the marketplace by SMTP.

This has left X.509 adrift. The original concept had called for a global top-level CA, perhaps administered by the United Nations, which would sign the keys of national CAs; these in turn would certify the keys of lower level CAs, and below this there would be both corporate key hierarchies and encryption services provided to private individuals.

An alternative concept, promoted by companies like Microsoft and Netscape, cuts governments out of the loop and focusses instead on industry sectors. The top-level key in each application is provided by the software vendor, with its public component embedded in the application. Thus, for example, Microsoft's top level ('root') key would certify that VISA was a 'brand bindery', VISA in turn would certify its member banks, and they would then issue certificates to their customers.

This second model is being implemented in the specific context of the SET protocol for credit card transactions over the Internet, but it is turning out to be less than generally applicable. The reason is that the software vendors are unable or unwilling to certify the top level keys of all the organisations that wish to become or to establish CAs. Thus one finds a small number of X.509 CAs whose root certificates are shipped with products such as Netscape Communicator and Microsoft Internet Explorer; but a large number of CAs find themselves excluded. This is especially a problem for CAs outside the USA.

It is also a problem for professional practice. Lawyers, doctors and other professionals tend to be organised either locally or nationally (and in the latter case often by speciality), with no effective supranational organisations that could take over the registration function of a 'brand bindery'. We are beginning to find numbers of small CAs springing up to certify keys in specialised networks; we include a number of them in this book, ranging from an EU project to replace bills of lading throughout Europe to a scheme to share radiology images between five London hospitals.

One systematic solution that has been suggested is that CAs should cross-certify each others' keys. However, the larger CAs are commercial competitors and so do not want to promote each others' business, while the smaller CAs have little reason to interact; for example, a London radiology CA has no obvious motive to establish relations with a CA serving patent attorneys in New Zealand. In addition, the certification policies of these different entities are often incompatible. So cross-certification appears to be of limited value, at least for the time being.

An alternative approach to the hierarchical model of CAs is given by Pretty Good Privacy (PGP), in which users certify each others' keys in a 'web of trust'. The problem here is that the web of trust is very patchy and uneven; while there are well-connected components (especially of computer security professionals) there are groups of PGP users who form isolated components and many individuals who are not connected at all. As with small CAs, there is little reason to expect that different specialities will be connected (indeed, small CAs are often implemented using PGP technology rather than X.509). Furthermore, it is not clear what trust can be placed on a chain of introductions, given that trust is not transitive.

The upshot of this historical legacy is that there is no cheap and effective way for Internet users to check the validity of public keys on which they may wish to rely. A US user, for example, cannot easily check the validity of a certificate from a server in the Czech Republic, if this is issued by a Czech CA whose root certifi-

cate is not included in the user's browser. She may just accept the certificate into her registry but it might have been issued by anyone!

We are trying to solve this problem by making available in this book the fingerprints or other information by which the root certificates and keys of the X.509 and EDI CAs known to us can be verified, as well as a number of the more important PGP keys used in the web of trust and elsewhere. When downloading such a certificate or key, you can have your browser or PGP software compute the relevant fingerprint and compare it with the value in this book. This should enable you to get a higher level of assurance of the key's authenticity that would otherwise be the case.

1.2 Grounding Trust in a Paper Book

One reason to favour a printed book for the global root CA is that the security issues for a book are much clearer and more tractable than for an electronic service based on a root certificate embedded in common browsers.

By far the simplest attack on a book is to manufacture a forged copy of it with one or more critical entries changed, and supply it surreptitiously to the target of the attack. Users can defend themselves against such an attack by purchasing their copy of the book either directly from the publishers (see details below) or from a randomly chosen bookstore. With particularly critical trust decisions, they may double-check against another copy of the book held in a local library, or against a copy on the shelf of a bookstore.

More pernicious attacks on a book include hacking into the editors' computer system, or the publishers' computer system, and introducing errors either to cause a false key to be accepted, or to undermine public confidence in the whole operation. We have taken reasonable precautions to prevent such attacks, although we cannot exclude them entirely; and it is in the nature of things that typos and other errors will occur. The nature of the checks we have carried out, the residual risks, our disclaimers, and the way in which trust in this product will be developed over time, are all set out below.

However, trust issues are straightforward in book publishing compared with the problems of running an electronic CA, and especially one at the root of a global system. An enormous variety of attacks may be mounted on computer systems — ranging from high-tech attacks such as cryptanalysis and Tempest through the exploitation of chance vulnerabilities in operating system and network software through to subversion of personnel and 'legislative' attacks such as requiring that CAs hand over keys to the government on demand.

In consequence, an online CA that were to serve mutually distrusting governments would be exceptionally difficult to construct; indeed we really have no idea how to do this technically. The repeated attempts to secure government access to CA and other keys (some of which involve dubious deals between equipment manufacturers, software vendors and governments) suggest that the problem of creating global trust in systems is probably a political impossibility as well.

By contrast, trust in a printed directory is relatively unproblematic because of the very long period over which trade directories, telephone directories, public registers of doctors and lawyers, and books of bankers' specimen signatures have been used in everyday life.

There are also legal considerations. A number of jurisdictions from Germany to Utah have adopted digital signature laws, while lawyers in some other jurisdictions aver that digital signatures are already valid under laws which define the essence of a signature as intent. Whatever the relative merits of these new laws and reinterpretations of old laws, the point is that they differ. So if a global top-level CA were to be instantiated in an electronic system, there would be enormous scope for confusion; it might be acceptable in some jurisdictions but not others, or have different force in different places. Thus, for a long time, there will be value in having a public register by which root CA certificates may be authenticated, and which escapes much of this legal morass by virtue of being implemented in ink and paper rather than software and hardware.

From the point of view of resilience, the fact that systems fail (and in particular the chaos forecast with the year 2000 date rollover problem) makes it prudent to have fallback paper mechanisms for critical procedures. Thus, even if a global electronic CA were to exist, something like this book would also have to be created as an emergency backup.

Finally, there are much less tangible cultural aspects to trust. Even among computer scientists (and security experts) there are still many people who trust paper documents over electronic ones; and in the lay population, who are exposed almost daily to scare stories about the insecurity of the Internet, paper is far more trusted. It is our hope that the publication of this book can start the process of transferring trust from the world of paper to cyberspace.

1.3 Scientific and Engineering Aspects

The exercise of collecting a large number of public keys highlighted several problems in currently implemented trust services, including both X.509 and PGP.

1.3.1 X.509

The most common software used to handle certificates nowadays is the web browser. There are several problems related to the common browser implementations and we give here an overview of the most important shortcomings.

Lack of transparency: when users download a copy of a browser, they get numerous different certificates that are supposed to be trusted and which are already embedded in the software. When they get a chain of certificates from somewhere on the net and need to verify it in order to authenticate a server (for example), the browser will perform the verification and will report at the end of the check if the verification has been successful or not. From the security point of view, this is not enough since users need to know also which, among all the CAs in the browser, they had to trust in the process. Users

might not trust all the hard coded CAs, or they might associate different levels of trust with them.

Lack of information: the common browsers do not display all the information used for computing the fingerprint. The fingerprint of the X.509 certificates listed in sections 2 and 3 is the MD5 hash of the DER encoding of the whole certificate. With some browsers, it is not possible to find an official copy of the hard coded root certificates, whether in the browser itself or on the relevant CA's web site. It is easy to find a fingerprint of the certificate, but requires considerable skill and effort for users to verify its correctness with their own implementation of the hash algorithm. This forces users to place a quite unnecessary level of trust in the browser, and increases vulnerability to attacks in which malicious code or other technical tricks are used to corrupt the browser's operation. (Our web page provides the missing information.)

Lack of standards compliance: browser manufacturers claim to display X.509 certificates but omit some mandatory fields. Microsoft Internet Explorer 4.0 does not include the serial number, despite this being mandatory and used to implement certificate revocation lists. Netscape Communicator 4.03 does not provide the right validity period: the hour and minute are missing while in the standard they are mandatory. Neither browser specifies the version or signature algorithm fields, and neither displays all the extension fields present, but only those fields defined by their vendors. This is a serious problem as extension fields are often used for access control decisions, and this misfeature prevents their being displayed and examined when the certificate is checked. This could allow unauthorised access to systems, or lead to owners of certificates being granted rights they have never asked for and thus assuming unwanted liability.

Dependency on browsers: some CAs have hard-coded different certificates for the same key and the same subject, but with different expiration dates, in different browsers. This practice could lead to some dangerous and dubious situations. What happens if a user successfully verifies a public key with one browser, and at the same time the same public key appears expired with another browser? Which copy of the certificate or of the browser should users believe and why? Having different certificates for the same subject name can cause confusion, because the fingerprints displayed by the browser for those two certificates are different while the key is the same.

This problem arises from the overlap of two different concepts: a certificate and a public key. In X.509, which all browsers claim to implement, the cryptographic credential used to identify a principal is the whole certificate rather than just the public key. Another disadvantage of having different certificates in different browsers is that users may need to request a different certificate from the same CA depending on their choice of browser. An unnecessary dependency between certificates and software is thus created.

Aggregation of trust at key generation: Using the browser to generate the key pair and submit a certification request to a CA may help in rapid deploy-

ment of the technology but is less than ideal. Suppose the CA's policy is that when it receives a certificate request it will have a staff member who knows the customer call her by telephone and verify the fingerprint of the public key (this might be the reasonable procedure where the CA is a professional practice such as a doctor or lawyer). However, the current browser implementations of key generation do not let the user see either the newly generated public key itself or its fingerprint. The fingerprint is also useful in other protocols that can be used to prevent middleperson attacks.

One solution to these problems is to have separate software for key generation. There is no engineering reason to create a strict dependency between the generation of users' certificates and the software they use it with. On the contrary, the general robustness of protection systems would be increased if users could choose from a range of vendors of key generation software, certificate management software, email encryption software, digital signature software and browser software. Such unbundling would tend to localise failures and to force interfaces to be transparent and well-documented.

Problem with root key revocation: some CAs have decided to hard code their root certificate in user software, even where the lifetimes of certificates and software are different. This can cause software to self-destruct at a given time in the future, a situation not unlike the 'millennium bug' of year 2000 rollover. If software persists past its design lifetime, or if the private part of the root key is compromised, then it becomes necessary to change the root public key in all the copies of the software. This could be a difficult and complex task, especially if the software is no longer maintained. Introducing such vulnerabilities without a very good reason is foolish, and 'planned obsolescence' for marketing purposes is not a good reason. Systems often persist for decades past their design lifetime, a good example being all the 1960's COBOL that still forms part of mission critical systems and whose maintenance is now a serious problem for many organisations.

Implementation defects: browsers, like other software, may contain bugs. For example, Netscape Communicator v 4.03 reports the expiry date of the MCI CA certificates as the 17th July 1998, rather than the 16th July 1998 as appears in these certificates. However the Belsign Class 1–3, which also expire on the 16th July, appear to be handled correctly.

1.3.2 PGP

For PGP keys, unlike X.509 certificates, there are already several sites that keep a public copy of the global `pubring.pgp`, so called a PGP key server.

Although these services are useful, they have lots of security holes. For example, one finds keys with names such as '`president@whitehouse.gov`' which bear no relation to the individual that one would naturally associate with that name. In fact, PGP key servers simply collect all keys sent to them, and verifying their authenticity is up to the user.

Users are supposed to verify keys either by means of a non-electronic channel (such as by meeting the keyholder in person and exchanging key fingerprints) or by means of a chain of introductions, in each of which one user signs another's key in order to certify his identity. These chains of introductions make up the so called 'web of trust'. However this web is at best patchy, and although it is easy to verify the keys of some people via multiple independent chains, there are many others for whom such authentication is problematic or impossible. By including a number of important PGP keys in this book, we hope to improve this situation somewhat.

The criteria we used to decide which PGP keys to include, and the various levels of care with which keys have been authenticated, are described below. Meanwhile, we will observe a technical weakness of PGP: that key fingerprints are computed on the concatenation of the RSA modulus and exponent. Thus the key with modulus `2E27...A1E733` and exponent `11` has the same fingerprint as the key with modulus `2E27...A1E7` and exponent `3311`. For this reason, a PGP key is not uniquely specified by its fingerprint, but by the combination of fingerprint and keylength.

Finally, there are a number of common problems with X.509 and PGP, whose scope we are only beginning to understand. One concerns the lack of global naming conventions. As an example, the AT&T X.509 root certificate has the distinguished name 'Certificate Services'. This is clearly not unique (neither is it an isolated example). We follow the Netscape interpretation and list this as 'AT&T Certificate Services'; one must however beware that MS Explorer lists it under the name 'ATT Certificate Services.' On the PGP side, the most common cause of failure was changing e-mail addresses.

A more serious problem with all the certification mechanisms is the widespread lack of operational robustness. Organisations trying to authenticate their keys to us have made just about every conceivable mistake: they have sent us the wrong keys, sworn to the wrong fingerprints, produced wrongly dated certificates, and have been unable to generate certificates with requested contents. Often the mechanisms just cannot be made to work at all. At very few sites have we found staff to be in control of their systems in the way that one expects, for example, in an office issuing passports or drivers' licences. Much of this clumsiness is no doubt due to the relative newness of the technology; but a very much higher level of robustness is required in implementations if the promise of public key technology is to be realised.

1.4 Politics

Some countries, such as the UK, have proposed government licensing of encryption services; a certification authority would be permitted to trade only if it escrowed its users' private confidentiality keys and made them available to the authorities on demand. Such a crippled certification authority is commonly known as a 'trusted third party' (the name chimes well with the NSA definition of trust, namely that a trusted system or component is one with the power to break

one's security policy). The European Union, on the other hand, opposes national trusted third party regulations that would impede either the trade in encryption products and services, or electronic commerce in general; and various other international bodies have emphasised the need for electronic trust services that can be relied on.

Given the determination of some national intelligence agencies to obtain access to cryptographic keys used in industry and commerce, this debate is unlikely to be settled in the immediate future. One of the contributions of this book is to present an implementation of a certification authority that, on the one hand, is a paper book and thus protected by the constitutions and bills of rights of various nations, while being on the other hand an 'encryption service' in terms of the previous UK government's proposed legislation and thus liable to licensing. We undertake that under no circumstances whatsoever will we apply for such a licence; should this book be banned in the UK by future escrow legislation, then the entire publication process will be shifted to the USA or elsewhere.

We would point out that basing commercial and professional trust on printed directories has a long history. Examples that come to mind include the Medical Register, the yellow pages, the many specialised trade directories, and the books of managers' signatures that banks print and send to other banks with which they do business. A government that banned our trust register should logically ban these books as well.

1.5 How We Chose and Checked the Keys

We have included the X.509 and EDI keys of all certification authorities known to us who have made their public keys available, whether by giving them to us, by publishing them or otherwise, and all PGP public keys which have been used to sign a significant number of other keys or which are used in certain defined roles (as top-level certifier keys, by webmasters, software distributors or computer emergency response teams).

Where possible we have carried out independent checks on the authenticity of each key, and the keys are marked from **D** up to **A** depending on the level of verification that we were able to carry out.

The definition of these levels of trust is as follows:

D means that we have no reason to believe that the principal who owns the key is other than as stated. We also have no particularly strong reason to believe the principal is as stated, so the level of assurance given by this level is vestigial. (Its main function is that, if the key remains unchallenged for some time, then it might acquire a slightly higher rating in future editions of this book.)

C means that the key has been certified by someone whose key we rate at B, or (for the majority of PGP keys in the book) that we verified the binding between the key and the email address by sending email, encrypted under the key, to the address and getting a signed response. In the case of X.509 certificates, we sent a cleartext email to an address found on the web site whence we down-

loaded the certificate, and asked for the postal address and/or the CA root public key signed by the CA root private key or by a key directly certified by the CA root key. Both of these methods of verification can of course be overcome by someone with the ability to forge email; but a similar procedure is used by commercial CAs for low-assurance consumer certificates. In our case, we sent out a large batch of encrypted emails with no prior publicity, so the likelihood of attacks involving a temporary takeover of a user's email address is low, and the level of assurance attained is reasonable (though not watertight).

B means that our knowledge of the binding between the key and the listed name rests on an introduction by someone we consider trustworthy and competent; if this introduction was effected using public key cryptography, then it used a key we rate at level A. (We apply a general rule that introduction cuts the trust level by one, so a key certified by a key at level B will have level C). We also set at level B those keys whose owners have authenticated themselves thoroughly by methods relying on formal government certification (such as by presenting passports, certificates of company incorporation etc) and by use of multiple conventional authentication mechanisms (such as when we telephone a switchboard number found in a telephone book, ask for a responsible person by role rather than name, and then confirm the key fingerprint by a protocol involving registered mail).

A means that at least one of us* has definite personal knowledge that the key belongs to the person or entity listed. Examples are the keys of colleagues and of well known companies whose root keys we have been able to verify by strong means (e.g., we dug out the key from the company's software and had it independently certified by at least one appropriately senior employee who has been known to us for a long time). Thus grade A keys are certified by more than formal processes; the position of the key owner in the social structure has been verified.

The arrangement of the keys into chapters has of necessity been rather ad hoc and depended on the numbers of keys of various kinds which we have received. In the medium to long term, we expect to see separate chapters for general CA services and for various business sectors such as banking, insurance, healthcare, education and so on; for the time being, there are only a handful of online players in each sector, and so we felt it not worthwhile to have many chapters with only two or three entries in them.

It would have been possible to have a separate chapter for universities but we decided against this for the time being as a significant number of university CAs (especially in the X.509 world) have been funded as joint ventures with industry. We have included a short separate chapter of medical keys, both as an experi-

* By 'us' in this context, we mean the six editors of the 'Global Trust Register' and two contributing editors: Johann Bezuidenhoudt and Markus G. Kuhn. We recruited Johann for his knowledge of South African CAs and Markus for his knowledge of German CAs.

ment and to support various pilots and projects in medical telematics. We trust that the number and size of such chapters will increase rapidly.

The largest single collection of keys we have is PGP keys. We thought it useful to partition these into three separate chapters — one for PGP keys used as institutional CA keys (including computer emergency response team keys), one for personal keys, and one for anonymous remailers (as the nature of trust here is somewhat different).

1.6 Disclaimer

We accept no liability at all for any errors in the entries in this book — including omissions and attacks. We do not believe that we have managed to publish the first book free of typos, or that the software we have written is the first program to be free of bugs. We believe that we have taken reasonable care, with all entries checked by a second individual; however we have not had the time or other resources to take extreme precautions against common-mode errors or attacks (for example, on our shared file system). We have also been limited by the data and resources available to us, and in particular by the responses from people and companies contacted. We believe that this situation will improve with time.

The purpose of this book is not due diligence but risk reduction. We aim to help a prudent person check the validity of certificates that are presented to him electronically; we do not aim to provide the only such means, still less to provide protection against the very large number of things that can go wrong with computer systems, or be utilised maliciously by an attacker.

Note that those real-world certificates which can be shown to an unlimited number of people, such as passports, birth certificates, driving licences and university degrees, are generally issued by organisations that will not accept liability for errors or forgeries. On the other hand, certificates which convey financial value (such as credit cards) are restricted in their use. A cardholder who emailed his credit card number to a hundred thousand online merchants in the space of an hour would incur the displeasure of his card issuer!

The kind of trust service provided by this book is solidly in the former category, and should be compared to printed registers of the members of restricted professions such as doctors or lawyers. Although such registers have mistakes in some entries, they still perform a useful service. Our book should be used in this light; failure to find an expected entry, or the discovery that an entry has an unexpected value, does not constitute proof of wrongdoing but simply indicates that closer attention is called for.

It should also be noticed that the great majority of commercial CAs have lengthy disclaimers and policy statements to the effect that they will not accept any liability either. Thus even if an entry in this book is correct and verifies that a certificate was issued by a given CA, and that CA certifies a key as belonging to a certain merchant, no particularly strong conclusion can be drawn. Hopefully this may change over time.

Where it is necessary to be able to place legal reliance on a digital signature, this commonly entails application specific mechanisms such as those in the Bolero system for bills of lading and in the proposed SET system for credit card transactions on the net. It is prudent for users to make themselves familiar with the terms and conditions under which each particular application operates; it is these terms on which users must rely when something goes wrong.

Finally, we want to emphasise that this first edition of the Global Trust Register is still experimental and should be considered a 'beta' release. Compiling it has enabled us to understand more thoroughly the engineering problems with various public key mechanisms, to develop and debug the software used to manage and format our key database, and perhaps most importantly to understand the logistics and procedural issues involved in running a global certification service.

1.7 Next Version

We have an outline agreement with MIT Press that they will publish the next (1999) edition of this book, which will be available at the end of 1998. We expect that the book will be greatly expanded and that the mechanisms for assuring trust in keys will be refined. The deadline for entries is the first of July 1998.

Errata will be made available from time to time on:

http://www.cl.cam.ac.uk/Research/Security/Trust-Register/

and at other mirrors to be arranged; they will be signed by three or more of us except in an emergency.

1.8 How to Buy a Copy

This book is distributed free with 'Computer and Communications Security Reviews', for which a subscription form can be found on:

http://www.cl.cam.ac.uk/~rja14/#SR

It can also be ordered direct from the publishers for £15.00 including airmail postage. We can accept email credit card orders, but some card issuers insist that your card number and expiry date be encrypted. You can use PGP; a key with fingerprint

E5 C7 93 BE : 37 9D 28 42 : : 49 DC A8 09 : A1 47 05 F6 1024

can be fetched from:

http://www.cl.cam.ac.uk/~rja14/

You can also fax your order to us on +44 1223 334678, or mail it to us at Northgate Consultants Ltd., 10 Water End, Wrestlingworth, Bedfordshire SG19 2HA, England.

Ross Anderson
Ross.Anderson@cl.cam.ac.uk
http://www.cl.cam.ac.uk/~rja14

E5 C7 93 BE : 37 9D 28 42 : : 49 DC A8 09 : A1 47 05 F6 1024
AF 5E F0 DF : 70 E3 E6 5B : : 66 D8 86 48 : 62 A1 E9 0A 2048

Bruno Crispo
Bruno.Crispo@cl.cam.ac.uk
crispo@di.unito.it
http://www.cl.cam.ac.uk/~bc201

1A D1 4A 1C : EE DD 32 D9 : : EC 5F 0C 93 : 17 C1 C6 5D 1024

Jong-Hyeon Lee
Jong-Hyeon.Lee@cl.cam.ac.uk
http://www.cl.cam.ac.uk/~jhl21

51 7B 32 A5 : 08 FA 8D B2 : : 3F 7B DA 8C : 73 17 95 15 1024
43 A2 6D 53 : 15 7C 88 1E : : E2 C2 A8 4B : D5 DE 78 D0 2048

Charalampos Manifavas
Charalampos.Manifavas@cl.cam.ac.uk
http://www.cl.cam.ac.uk/~cm213

D4 BF D5 6C : 86 83 EC 37 : : 88 B1 8E 92 : 9D 9A 97 FA 1024

Václav Matyáš Jr.
Vaclav.Matyas@cl.cam.ac.uk
matyas@informatics.muni.cz
http://www.cl.cam.ac.uk/~vm206

C3 CB 4E FD : 9E DE F0 CA : : 65 D5 BF 7C : 46 8F 7B 5C 1024
B9 B3 F9 AA : E5 1B 38 0E : : F9 DF 00 21 : CA F6 87 57 2048

Fabien Petitcolas
Fabien.Petitcolas@cl.cam.ac.uk
http://www.cl.cam.ac.uk/~fapp2

27 09 EB 53 : 98 99 B2 8B : : CA DB AC 31 : CC FD 2B 1B 1024
24 61 2F 47 : DB 04 27 DD : : 8E 6F 76 60 : 5A 24 20 45 2048

2 Certification Authorities

Ad Aequitatem INFOSEC
Ad Aequitatem
Spain
https://www.siscer.com/adaequitatem.cacert
1E 42 55 DA : 74 DD 3B 7C : : 72 4D 9C 44 : 13 6E 0A B0
D
08 May 1998

Asia Public Certificate Authority
Hong Kong, China
csr@asiaca.org
http://sun.cary.net/CA/

Asia Certificate Authority - Hong Kong
94 34 8F B7 : 3E A6 3B 34 : : 1F 75 83 82 : E0 54 6A C6
D
21 Jun 2017

AsiaCA Root CA Certificate - Hong Kong
E9 DA 10 3F : 07 42 3D DF : : B8 B6 0C 43 : 50 26 25 84
D
26 Jun 1998

AT&T
USA
http://www.att.com/

AT&T Certificate Services
34 FA BD 73 : DB 25 C5 54 : : 33 A2 AB B3 : 27 5F 2A 84
D
31 Dec 1999

AT&T Directory Services
4C FC FD DD : DF AC 7E 14 : : A5 0A DE 0B : F5 38 9D AC
D
16 Jan 2001

Baltimore Technologies CA
Baltimore Technologies Ltd., IFSC House.
Custom House Quay. Dublin 1. Ireland
Tel: +353 1 605 4399
Fax: +353 1 605 4388
info@baltimore.ie
04 FA 2E DF : 60 7E 9D 27 : : 17 A1 41 FC : EE C9 80 ED
A
29 Sep 1998

BBN Certificate Services CA Root 1
BBN Certificate Services
USA
http://www.bbn.com/
A1 FB 06 83 : 8A 10 0D 6B : : C9 58 81 D9 : C2 92 C2 59
D
25 Dec 1999

BelSign NV
Brussels, Belgium
webmaster@belsign.be
http://www.belsign.be

BelSign Secure Server CA
DB 38 25 7E : C4 CE FF 62 : : 13 4D 5F 13 : F5 A4 E3 B2
D
15 Jul 1998

BelSign Class 1 CA
A7 48 93 0A : 64 AD 98 E0 : : FA 5B 5A BE : 6F 29 F1 68
D
16 Jul 1998

BelSign Class 2 CA
77 A9 F0 33 : 6B A7 9F 6D : : 46 B7 A9 3A : 64 9E B7 31
D
16 Jul 1998

BelSign Class 3 CA
9A B6 64 18 : 02 CF 7E 98 : : 6D 87 DF 07 : 4B 48 E9 06
D
16 Jul 1998

BelSign Class 1 Public Certification Authority
class1@belsign.be
B8 A0 82 E1 : 1E D8 65 11 : : 66 3F 34 D8 : C8 81 03 2F
D
4 Oct 1999

BelSign Class 2 Public Certification Authority
class2@belsign.be
BF 60 C3 3E : 31 8E B1 88 : : 5D 02 71 04 : B3 24 5C 47
D
4 Oct 1999

BelSign Class 3 Public Certification Authority
class3@belsign.be
33 66 8E A6 : 30 52 C5 0E : : F0 AF A2 96 : 5A B8 31 C8
D
4 Oct 1999

BiNARY SuRGEONS CA
BiNARY SuRGEONS
Johannesburg, Gauteng, South Africa
certificates@surgeons.co.za
http://www.surgeons.co.za/cert/
0E C0 09 EC : 7A C0 8E 1C : : 25 24 C7 54 : DC 73 AB 20
D
25 Oct 2000

BizNet CA
BizNet Certificate Services, BizNet Communications Inc.
St.Louis Missouri USA
http://www.biz1.net/biznet.cacert
C1 2A 7E 21 : 2C 19 FD BF : : 87 81 0F 13 : 0C 10 C8 54
D
16 May 1999

Brook Schofield Consulting - CA
Certificate Services Division
Brook Schofield Consulting
Launceston, Tasmania, Australia
Brook@CUSAeeMe.educ.utas.edu.au
4E 9C 68 05 : DA 63 AA E3 : : 8B 9D C9 ED : B9 71 CC 1B — **D** 10 Jul 1998

Canada Post Corporation CA
Canada
44 A2 FF F8 : 64 8D 81 80 : : A0 39 83 5B : 84 1A F3 75 — **D** 27 May 2016

CertiSign BR
CertiSign Certificadora Digital Ltda
Brasil
http://www.certisign.com.br/
82 DC BF 51 : 6E E3 9E F3 : : 96 7C 60 6D : A6 6C FC C8 — **D** 31 Dec 1999

Columbia University CA
Columbia University
New York City New York USA
cert-auth@columbia.edu
http://www.columbia.edu/
18 CE C6 6B : 2C 41 4A 75 : : 15 F1 93 FB : 29 04 00 8F — **D** 28 Apr 2000

COST Top Level CA
Computer Security Technologies CST AB
Stockholm, sweden
http://www.cost.se/pca.htm
B9 9C C8 1A : 59 6B 2E 93 : : 80 7E DA 25 : 49 58 A6 33 — **D** 19 Sept 1998

DataNet Intranet Certification Authority
DataNet a.s.
Chlumcanskeho 5, 180 00 Praha 8, Czech Republic
webmaster@datanet.cz
http://www.datanet.cz/certifik.html
39 1A C6 E3 : 3F 98 D7 96 : : 52 AA 90 37 : 90 43 CD 01 — **D** 16 Feb 2002

Denmark CA
ICE-TEL Project, UNI-C
Vermundsgade 5, DK-2100 Copenhagen, Denmark
Tel: +45 35 87 88 89
Fax: +45 35 87 88 90
dk-ca@uni-c.dk
http://ice-tel.uni-c.dk/dk-ca/
F4 5C 31 6C : DC EC 2E 49 : : 11 53 1F AE : D7 0A 32 8B — **D** 31 Dec 1999

Deutsches Forschungsnetz
DFN-PCA, Universität Hamburg, Fachbereich Informatik
Vogt-Kölln-Straße 30, D-22527 Hamburg, Germany
Tel: +49 40 5494 2262
Fax: +49 40 5494 2241

Deutsches Forschungsnetz - ICE-TEL PCA
http://www.pca.dfn.de/dfnpca/certify/pem/userca.der
16 05 C2 A9 : 29 76 E9 B8 : : 6C A7 91 7C : 3B 58 3E 75
D
31 Dec 1998

Deutsches Forschungsnetz - PCA (Low-Level)
http://www.pca.dfn.de/dfnpca/certify/pem/pcalow.der
8C C6 1D 28 : 1B CB F9 3D : : 68 83 AC 02 : C8 3E FF 84
C
31 Dec 1998

Deutsches Forschungsnetz - PCA (Medium-Level)
http://www.pca.dfn.de/dfnpca/certify/pem/pcamid.der
0F BC 6D 29 : 4D A5 90 C1 : : D1 B9 D6 BD : 37 8F 2B 04
C
31 Dec 1998

Deutsches Forschungsnetz - User Certification Authority
http://www.pca.dfn.de/dfnpca/certify/pem/userca.der
A9 1A 6F A4 : 23 E7 F0 E7 : : 4F 67 39 37 : 01 9E 6B D0
D
05 May 1998

EEPO
EEPO Pty Ltd
Australia
security@eepo.com.au
http://www.eepo.com.au/security/
D6 5B 0D 15 : 23 FB EF BE : : 83 1B 63 A0 : 3C 95 1E 06
D
29 Oct 1998

Entropia Class 2 Public Primary CA
Entropia Internet CA
1038 Corvette Drive, San Jose, California 95129-2903 USA
Tel: +1 408 255 2388
webmaster@entropia.com
http://entropia.com/ca/
63 1D DF 9A : C7 0B 28 DE : : 44 7C 1B 77 : 74 83 A8 86
D
30 Jun 2000

Equitable Life Certificate Authority
The Equitable Life Insurance Company of Canada
Waterloo, Ontario, Canada
http://www.equitable.ca/network.html
9C AF 4A A7 : A4 98 9A 83 : : D3 8C B6 04 : 2E A4 62 E7
D
11 Apr 1999

Estonian Card Centre of Banks Certificate Authority
Certificate Authority, Card Centre of Banks
Tallinn, Estonia
http://www.hansa.ee/certs/cc-ca.cert
ca@estcard.ee

60 40 B6 49 : A2 C0 F8 99 : : 22 CB 3C 68 : E4 86 F4 13 — **D** 01 Jun 1998

EuroSign
EuroSign
United Kingdom
http://eurosign.com/help/eurosign/certinfo

BA 35 AF 21 : A7 EF DC 0D : : 2C 77 54 BC : CC 7A 9D FD — **D** 30 Oct 2002

GTE Corporation
USA
http://www.cybertrust.gte.com/

GTE CyberTrust Root CA

22 47 D0 75 : 47 5C 43 08 : : 52 6A 2C F3 : 3E B1 53 5B — **D** 31 Dec 1999

GTE Secure Server CA

E6 77 D7 5A : 16 B8 D1 66 : : D5 96 06 3B : 7D D2 EB 1C — **D** 30 Dec 1999

GTIS/PWGSC, Canada Gov.
Government of Canada
Canada
http://www.cse.dnd.ca/cse/english/gov.html

GTIS/PWGSC, Canada Gov. Secure CA

C0 85 54 7B : 39 35 5A FE : : 24 3E 69 AE : C0 BE B9 85 — **D** 25 Apr 2017

GTIS/PWGSC, Canada Gov. Web CA

E5 33 E1 2B : 54 08 B8 CC : : DC A2 B5 AE : 98 82 D3 9E — **D** 14 Feb 2002

IBM World Registry CA
IBM World Registry
USA
http://www.ibm.com/

7C 73 0A 91 : E2 FF 94 34 : : 93 36 FE B0 : 35 30 82 4F — **D** 20 May 2017

ICAT Certification Authority
Japan
http://www.k-isit.or.jp/dccf/

B6 0A 38 A2 : EF 1A 20 6C : : 4E 9B BA 79 : 8B 8C AC 77 — **D** 10 Jan 1999

ICE-TEL Top Level Certification Authority
ICE-TEL, UNI-C Copenhagen
Vermundsgade 5, DK-2100 Copenhagen, Denmark
Tel: 45 35 87 88 89
Fax: 45 35 87 88 90
ice-ca@uni-c.dk
http://ice-tel.uni-c.dk/ice-ca/
91 C6 4D F2 : DE F6 DF C2 : : BC 9D BF 7D : 71 2F 07 50
D
31 Dec 1999

IKS GmbH
Jena, Thuringia, Germany
ca@iks-jena.de
https://www.iks-jena.de/produkte/ca/index.en.html

Hohe Sicherheit (SIGN)
84 F8 C0 23 : 5C 40 BB 48 : : 03 8A 6D 19 : 7F 2E F5 5F
B
29 Apr 1998

Niedrige Sicherheit (SIGN)
00 12 31 02 : F1 B6 DD B5 : : F5 34 1C 87 : EB FF 8D 28
B
29 Apr 1998

Integrion CA
Integrion Financial Network
USA
C4 51 2D B7 : 2C DF AC CE : : E1 AA 42 8D : 6D DC 9E 4D
A
20 May 2017

Intercomputer S.A. - SISCER
Intercomputer S.A.
Zaragoza Spain
http://www.siscer.com/siscer.cacert
AE D1 C7 8B : C3 04 D4 58 : : 2C 9B 2F 7D : 49 ED 94 A4
D
14 Mar 1998

Internet PCA Registration Authority
Internet Society
http://bs.mit.edu:8001/ipra.html
12 2F 1C 5F : 5E DA 6E EC : : 49 5A 9E BA : FF 3A 48 61
D
15 Sep 1999

IPS CA Servidores
Certificaciones, IPS Seguridad CA
Barcelona, Spain
ips@mail.ips.es
http://www.ips.es/
6E 7E 54 9A : 3B 6D 10 1F : : F4 89 CF AF : 26 8F EB FA
D
31 Dec 1999

ISIT - Certification Authority
ISIT:Institute of Systems & Information Technologies
Japan
http://www.k-isit.or.jp/dccf/

D
0A 3D FD C2 : E0 6B AF 57 : : 9E 63 F3 41 : 5C 79 37 C1 — 03 Apr 1998

KAIST Certification Authority
KAIST
Taejon, Korea
kaistca@kaist.ac.kr
http://camis.kaist.ac.kr/kaist-ca/

D
26 41 99 D2 : 1F DB 61 61 : : 0A 02 7B 43 : BB D6 E3 36 — 27 Feb 1999

Keywitness Canada Inc.
Canada
http://www.keywitness.ca/

for Microsoft Internet Explorer 4
D
FA 09 6C 1E : 99 80 68 27 : : 8E 63 30 30 : E6 5B F6 D1 — 07 May 1999

for Netscape Communicator 4
D
78 29 EC 13 : 15 D7 8B 46 : : 70 9B 47 92 : 4D 8B 6B 8E — 07 May 1999

Lemures CA
Lemures CA
Columbus, Ohio, USA
http://lemures.shinma.symix.com/myca.cacert

D
86 01 00 A8 : B2 42 92 1A : : FD CA E9 3E : 9E B1 47 A1 — 05 Mar 1999

MCI - internetMCI MALL
MCI
USA

D
79 F1 0A 61 : BD 32 F5 16 : : 12 D8 07 6B : 8D 9B A1 76 — 16 Jul 1998

Microsoft Corporation
USA
http://www.microsoft.com

Microsoft Authenticode™ Root Authority
A
DC 6D 6F AF : 89 7C DD 17 : : 33 2F B5 BA : 90 35 E9 CE — 31 Dec 1999

Microsoft Root Authority
A
2A 95 4E CA : 79 B2 87 45 : : 73 D9 2D 90 : BA F9 9F B6 — 31 Dec 2020

Microsoft Root SGC Authority
A
35 DB 26 52 : DB 79 9E B5 : : A9 14 90 0B : 94 EE 9C C9 — 01 Jan 2010

Microsoft Timestamping Service Root — **A**
55 6E BE F5 : 4C 1D 7C 03 : : 60 C4 34 18 : BC 96 49 C1 — 30 Dec 1999

MIT Certification Authority
Massachusetts Institute of Technology
Massachusetts USA
http://bs.mit.edu/mitca/ — **D**
BB 43 9C 06 : 0A 2C A2 EC : : BB 65 83 E5 : E0 84 B8 C6 — 13 Jul 2006

Multiboard Communications
Multiboard Communications HQ
London, Ontario, Canada
support@multiboard.com
http://www.multiboard.com/cacert.der — **D**
3C BA 74 EE : 7A 75 89 F9 : : 6F 83 BE 38 : F8 DF 11 9E — 22 Nov 1998

NUMNET CA - Fairfax County Employees Credit Union
USA
http://www.fairfaxcu.org/cacert.cac — **D**
01 5E 3F 75 : CB 0F 9C A8 : : E1 D8 F1 9A : B9 59 12 27 — 26 Mar 1999

Politecnico di Torino TrustFactory
ICE-TEL Project
Politecnico di Torino
Italy
http://www.polito.it/ice-tel/pca-it/ — **D**
C4 3F 92 09 : 34 0D E6 6B : : 47 71 20 12 : 74 EE 32 80 — 15 Dec 1998

PVT - 1.CA
PVT a.s.
Czech Republic
caoper@p70x03.brn.pvt.cz
http://www.ica.cz — **D**
12 AA 82 70 : A7 AD C9 0E : : 30 E3 2D 29 : 35 87 EB 3E — 17 Jun 1998

RSA Inc.
see VeriSign/RSA

Scalaire
Internet Certification Unit
Bordeaux, France
http://www.scalaire.fr/cacert.der — **D**
0B 7D 00 A3 : A0 DA B8 FF : : A2 FE 9B 3C : B5 81 58 8A — 27 Oct 1999

Slovenian Certification Authority (SI-CA)
ICE-TEL Project, Jozef Stefan Institute
Jamova 39, Ljubljana, SI-1000, Slovenia
Tel: +386 61 1773 639
Fax: +386 61 123 21 18
si-ca@e5.ijs.si
http://www.e5.ijs.si/cert/sipca_cert.html

Slovenian Certification Authority (SI-CA) Top Level Certificate — **D**
DD 12 0C 51 : EF 65 B0 F0 : : 25 AE 37 FA : AE 58 6F F4 — 31 Dec 1999

Slovenian Certification Authority for Individuals — **D**
B2 8F AE 0F : D7 33 3D EB : : BC 58 FA 41 : 8D 1B 6D F2 — 31 Dec 1999

Slovenian Certification Authority for Secure Web Servers — **D**
01 49 98 F9 : 25 3E 53 0D : : 6F AE 45 BE : 46 42 D8 60 — 31 Dec 1999

SIA CA
Societá Interbancaria per l'Automazione S.p.A.
Viale Certosa, 218, 20156 Milan, Italy
Tel: +39 2 3005 277
Fax: +39 2 3800 3333
santoni@sia.it
http://www.sia.it/clienti/siaca/siaca-nav.crt — **C**
61 DC EF 02 : FF B6 66 7F : : B3 65 04 CC : 30 12 A6 2A — 01 Apr 1999

SoftForum CA
SoftForum
Dongsuh Securities B/D 6th fl., 271-1 Suhyun, Boondang
Sungnam, Kyunggi-Do, Korea
camaster@softforum.co.kr
http://www.softforum.co.kr:4040/ — **A**
2C EF 03 C0 : 37 F6 48 FA : : EF 57 BB D1 : 2B 84 2D 75 — 31 Jan 2005

South African Certification Agency (Pty) Ltd. (SACA)
P.O.Box 8135, Centurion, 0046, Republic of South Africa
Tel: +27 12 665 0089
Fax: +27 12 665 0088
christi@caca.net
http://www.saca.net/

SACA Class 2 CA Certificate — **A**
EC 75 96 22 : 72 FC C6 0E : : 87 31 3A E9 : 09 8F AA EB — 19 Sep 1999

SACA Class 3 CA Certificate — **A**
65 4A 25 29 : 52 BF A4 80 : : 53 32 E8 32 : 45 A4 EC F4 — 18 Sep 1999

Systemberatung Axel Dunkel GmbH
Germany
http://www.ca.dunkel.de/

Class A Certification Authority — **D**
9F 0E E0 3D : DF A7 E9 5A : : 4C 5A 00 CF : 73 FB 76 0B — 31 Dec 1999

Secure Server Class B Certification Authority — **D**
2B 15 B8 40 : 67 61 E4 46 : : 5E E9 48 59 : 54 FC 75 78 — 31 Dec 1999

Thawte Consulting
South Africa - P.O. Box 2749 Durbanville 7551
USA - 6200 Falls of Neuse Suite 200 Raleigh NC 27609
personalbasic@thawte.com
http://www.thawte.com/

Thawte Personal Basic CA — **A**
E6 0B D2 C9 : CA 2D 88 DB : : 1A 71 0E 4B : 78 EB 02 41 — 31 Dec 2020

Thawte Personal Freemail CA
personalfreemail@thawte.com — **A**
1E 74 C3 86 : 3C 0C 35 C5 : : 3E C2 7F EF : 3C AA 3C D9 — 31 Dec 2020

Thawte Personal Premium CA
personalpremium@thawte.com — **A**
3A B2 DE 22 : 9A 20 93 49 : : F9 ED C8 D2 : 8A E7 68 0D — 31 Dec 2020

Thawte Premium Server CA
premiumcerts@thawte.com — **D**
9B 3B FD 23 : 6C 4B A0 4A : : 54 1C 7A 7D : 33 35 27 91 — 27 Jul 1998

Thawte Premium Server CA — **A**
06 9F 69 79 : 16 66 90 02 : : 1B 8C 8C A2 : C3 07 6F 3A — 31 Dec 2020

Thawte Server CA
servercerts@thawte.com — **D**
70 B4 B1 D3 : D3 99 EC 7E : : 94 68 C7 5C : C4 E1 02 1C — 27 Jul 1998

Thawte Server CA — **A**
C5 70 C4 A2 : ED 53 78 0C : : C8 10 53 81 : 64 CB D0 1D — 31 Dec 2020

TIN CA
Telecom Italia
Rome, Italy
webmaster@how.tin.it
http://security.tin.it — **D**
4F F2 1C F9 : A5 4D 66 E7 : : DD AE 8F 52 : AC 00 D5 6E — 30 Dec 1998

Tower CA
Tower SSL, Tower Network Design
Frankfurt/M., Hessen, Germany
root@tower.de
http://www.tower.de/towercacert.cacert
B0 D9 C5 7B : 41 63 73 C2 : : 59 01 A2 24 : 99 6A 31 20 — **D** 05 Jun 2000

TrustFactory Digital ID Services
ICE-TEL Project, GMD
Tel: +49 6151 869 715
Fax: +49 6151 869 704
support@secude.com
http://www.secude.com/trustfactory/trustfactory.htm

Class 0 Trial Services PKI
8A DB C7 FD : 89 1D 51 03 : : D3 32 24 DC : 93 58 D4 AA — **D** 1 Jan 2000

Class 0 Trial Services PKI - ICE-TEL
87 B6 49 A4 : FA 7F 58 72 : : 43 BF FD 1F : D7 53 64 FE — **D** 1 Jan 2000

Individual Subscriber Test Certificates
47 5A A5 71 : 8D F1 F8 F0 : : 21 13 A9 7E : 3B 77 1B CB — **D** 1 Jan 2000

Secure Server Test Certificates
98 30 DB D1 : 33 47 77 A1 : : 76 FE C6 B1 : 52 C3 F4 AA — **D** 1 Jan 2000

Uninett TrustFactory
ICE-TEL Project
Uninett
Norway
http://www.uninett.no/pca/index-e.html
DD 68 98 15 : 24 E7 5B 9A : : B1 BE 40 7C : 68 FD 5B C2 — **D** 10 Oct 1998

Universidade de Lisboa TrustFactory Digital ID Class1
Universidade de Lisboa
Portugal
http://science.di.fc.ul.pt/trustfactory/
D0 3C DB 00 : 09 EC 93 46 : : 4E C5 A4 C5 : 1B 04 0B ED — **D** 30 Apr 1998

University College London TrustFactory
ICE-TEL Project
UCL
United Kingdom
http://auchentoshan.cs.ucl.ac.uk:8877/trustfactory/
93 8B 7B 31 : 18 C1 E6 5B : : 15 51 98 1A : BE A6 E0 84 — **D** 22 Apr 1998

Uptime Commerce Ltd
Uptime Group Plc
59 Mansell Street London E 1 8AN United Kingdom
Tel: +44 171 481 1221
Fax: +44 171 481 1220
certs@uptimegroup.com
http://www.uptimecommerce.com/

Uptime Group Plc. Class 1 CA
85 1F 0A 65 : 74 43 24 2F : : A7 01 C8 71 : A4 95 D8 0F
A
21 Apr 2002

Uptime Group Plc. Class 2 CA
54 6A EA 11 : 24 BF 94 8B : : 0B 0A 17 60 : D8 35 B3 21
A
21 Apr 2002

Uptime Group Plc. Class 3 CA
DB E8 28 92 : 1A 70 8C 7B : : 88 7B C1 59 : ED A2 BB D1
A
21 Apr 2002

Uptime Group Plc. Class 4 CA
2D 1F C7 64 : 33 AC 18 97 : : B1 00 BB A3 : 93 23 09 A6
A
21 Apr 2002

VeriSign Inc.
1390 Shorebird Way, Mountain View, CA 94043, USA
Tel: +1 650 961 7500
Fax: +1 650 961 7300
practices@verisign.com
http://www.verisign.com/

VeriSign Class 1 Primary CA
00 EC 35 D1 : 64 A0 B9 24 : : 16 79 C0 64 : C1 06 48 84
A
31 Dec 1999

VeriSign Class 1 Primary CA
C0 E8 E5 2A : F1 CB E7 93 : : DB 9F 3A E5 : A8 E2 08 A1
D
7 Jan 2004

VeriSign Class 1 Primary CA
51 86 E8 1F : BC B1 C3 71 : : B5 18 10 DB : 5F DC F6 20
A
7 Jan 2020

VeriSign Class 2 Primary CA
E6 66 A4 8F : DA 51 DA 82 : : 74 C5 FB A4 : F0 0E A2 4F
A
31 Dec 1999

VeriSign Class 2 Primary CA
EC 40 7D 2B : 76 52 67 05 : : 2C EA F2 3A : 4F 65 F0 D8
A
7 Jan 2004

VeriSign Class 3 Primary CA
AC 46 90 6D : F9 38 74 ED : : 31 D4 C4 DD : ED 59 70 E4
A
31 Dec 1999

VeriSign Class 3 Primary CA
78 2A 02 DF : DB 2E 14 D5 : : A7 5F 0A DF : B6 8E 9C 5D
A
7 Jan 2004

VeriSign Class 4 Primary CA
1B D1 AD 17 : 8B 7F 22 13 : : 24 F5 26 E2 : 5D 4E B9 10
D
31 Dec 1999

VeriSign Commercial Software Publishers CA
E8 CC 9F B0 : 9B 40 C5 1F : : 4F BA 74 21 : F9 52 85 7A
D
31 Dec 1999

VeriSign Commercial Software Publishers CA
DD 75 3F 56 : BF BB C5 A1 : : 7A 15 53 C6 : 90 F9 FB CC
D
07 Jan 2004

VeriSign Individual Software Publishers CA
2B 50 87 18 : 39 2D 3B FF : : C3 91 7F 2D : 7D C0 8A 97
D
31 Dec 1999

VeriSign Individual Software Publishers CA
71 1F 0E 21 : E7 AA EA 32 : : 3A 66 23 D3 : AB 50 D6 69
D
07 Jan 2004

VeriSign Time Stamping CA
EB B0 4F 1D : 3A 2E 37 2F : : 1D DA 6E 27 : D6 B6 80 FA
D
07 Jan 2004

VeriSign/RSA
VeriSign, Inc.
1390 Shorebird Way, Mountain View, CA 94043, USA
Tel: +1 650 961 7500
Fax: +1 650 961 7300
practices@verisign.com
http://www.verisign.com
http://www.rsa.com/

VeriSign/RSA Commercial CA
5A 0B DD 42 : 9E B2 B4 62 : : 97 32 7F 7F : 0A AA 9A 39
D
03 Nov 1999

VeriSign/RSA Secure Server CA
74 7B 82 03 : 43 F0 00 9E : : 6B B3 EC 47 : BF 85 A5 93
A
07 Jan 2010

VeriSign/RSA Secure Server CA
11 56 32 B0 : C4 27 39 45 : : 8D 5C F4 41 : 89 5F 1C 72
A
31 Dec 1999

World Wide Wedlin CA
World Wide Wedlin
Linköping Östergötland Sweden
ca@wedlin.pp.se
http://www.wedlin.pp.se/ca/
8D 0A 39 6C : 0D 74 24 9E : : 0A 87 CB 97 : 4C E3 1D 76
D
10 Sep 2007

Communication Network Lab. - Taegu Univ.
Taegu Univ.
Kyungsan, Kyungpook, Korea
admin@altair.taegu.ac.kr
http://cnl.taegu.ac.kr/getca.html

D
24 Jul 1998

40 9C CB 2F : 0A F1 17 B2 : : 54 F2 31 04 : 50 0D AE 3E

3 Secure Web Sites

Apollo Advertising
Aylesbury Buckinghamshire United Kingdom
https://apollo.co.uk
1F 06 78 4E : F4 AB 48 B7 : : 45 B1 E4 F6 : 7A 42 5D A3
D
05 Nov 1998

Automated Transaction Services Inc.
Secure Services Devision
Sacramento, California, USA
https://www.atsbank.com
1B F6 8A 26 : D9 4E 5C 26 : : 56 2D 55 12 : 82 ED 4D 94
D
01 Jul 1998

Business Briefing Publishing Ltd
Web products division, www.businessmonitor.co.uk
London, United Kingdom
https://www.attica.co.uk/
17 34 4C FD : 49 4E 33 BF : : 40 54 C3 B4 : C7 48 FE AF
D
05 Feb 1998

CCS a.s.
CCS, a.s.
Praha, Czech Republic
https://bbs.ccs.cz
18 0C 6D ED : F7 0E 8A 4E : : B2 E7 76 BC : B1 92 17 20
D
24 Feb 1998

Columbia University Web Server
Columbia University
New York USA
webmaster@columbia.edu
https://www1.columbia.edu
75 C9 ED 53 : 06 14 B2 A4 : : A3 B8 1C 0F : D4 DE 71 78
D
02 Jul 1998

CU-SeeMe.educ.utas.edu.au
University of Tasmania, Faculty of Education
Launceston, Tasmania, Australia
www@CUSAeeMe.educ.utas.edu.au
https://cu-seeme.educ.utas.edu.au/Apache-SSL/
96 E4 2D EE : BF 5C 2D 19 : : 67 CB 15 67 : AD 59 44 E1
D
13 Jul 1998

Equitable Life of Canada
I/T, The Equitable Life of Canada
Waterloo, Ontario, Canada
http://www.equitable.ca/network.html
BD AD 49 CC : AB 7D 40 EC : : FA C1 31 1B : FD 73 6B B7
D
16 Oct 1999

Estonian Savings Bank
Public Relations
Tallinn, Estonia
webmaster@www.esb.ee
https://www.esb.ee
11 A4 85 F9 : 9E 63 53 BA : : FB CB 8D 6A : 33 4F 61 6C
D
31 May 1998

Fortis Bank Luxembourg
E-banking, Fortis Bank Luxembourg
Luxembourg, Luxembourg
https://www2.fortisbank.lu
07 F6 81 F4 : C5 E9 33 D2 : : 13 B9 13 18 : D8 56 62 18
D
31 Jul 1998

Hansabank
Tallinn, Estonia
https://www.hansa.ee/
96 F8 11 5B : 5D F6 3E 40 : : 83 AB 5F B6 : F3 47 2E 01
D
09 Jul 1998

Internet Direct, Inc.
*.direct.net, Secure Services Division
Internet Direct Inc.
Phoenix Arizona USA
ssl@gosite.com
https://www.tmsi.co.uk/
09 16 0D A6 : 68 7B CB 85 : : CF BB 0E 5E : C8 7F 1D D1
D
24 Apr 2000

IPS Internet
*.ips.es, Internet IPS
Barcelona, Spain
https://www.ips.es/
DA 67 6F 0A : 6D 8E CC 9D : : F1 91 4F 77 : 2E 72 11 96
D
28 Apr 1998

KAIST - CAMIS
CAMIS, KAIST
Taejon, Korea
webmaster@camis.kaist.ac.kr
https://camis.kaist.ac.kr/
61 A6 66 3A : 3E FF 20 8E : : 54 D0 6B 3C : 69 5C F9 A7
D
03 Mar 1998

Kathert: Hardware - Software - Neue Medien
Berlin, Germany
https://ccard.kathert.de
6B 5D A8 8E : E4 85 6D 0D : : C7 97 48 DD : EC F3 6E 02
D
24 May 1998

MARKnET Communications Electronic Commerce Services
MARKnET Communications
Boston Massachusetts USA
https://mall.marknet.com
36 F9 29 C2 : F0 C7 29 34 : : 21 32 C5 D7 : D4 65 36 F3
D
04 Nov 1998

Multiboard Communications
Multiboard Communications HQ
London, Ontario, Canada
support@multiboard.com
https://www.multiboard.com/home/register.html
1A F5 60 FC : 2E 48 29 40 : : C8 47 FF 76 : 48 D0 6B CE
D
22 Nov 1998

Paris Duty Free
Sales - Ventes
Paris, France
http://www.parisdutyfree.com/secure.html
0B 7D 00 A3 : A0 DA B8 FF : : A2 FE 9B 3C : B5 81 58 8A
D
27 Oct 1999

SavageS.com
Beaverton, Oregon, USA
ssl.savages.com
https://virtual.savages.com
7F F9 98 B1 : 9F 56 73 E2 : : 5D 07 99 81 : 11 44 14 58
D
02 May 1998

Squirrel Software Technologies Pty Ltd
Administration, Squirrel Software Technologies Pty Ltd
Queensland, Australia
http://www.squirrel.com.au/security/
58 A5 F7 2E BF 8C C4 2F 55 DE C0 19 9F 9D A4:9C
D
07 Feb 1998

Tower Network Design
Tower Mailbox, Tower Network Design
Frankfurt/M., Hessen, Germany
root@tower.de
https://www.tower.de
8D 9B B2 C9 : 7B 46 1B 67 : : EA B8 CE 3F : 2A A4 15 EB
D
09 Jun 1998

UK Web Ltd
Leeds West Yorkshire, United Kingdom
https://www.ukweb.com/
23 57 11 90 : 2E 99 F6 DB : : 68 21 F4 D9 : B7 AA 3A 5D
D
23 Sep 1998

Yellowpages Slovenia
Jasico d.o.o.
Murska Sobota, Slovenia
yellowpage@eunet.si
http://yellow.eunet.si
82 77 67 D7 : 62 9F E5 55 : : 6D AD DF AD : A9 A9 D7 1D

D
18 Jul 1998

4 EDI Keys

Public key techniques are used extensively in EDI systems. Most of these are private; in fact the Bank of England refused to publish the root key for CREST (the system used to register shares and other securities in the UK) as it is only 512 bits long.

However there are two EDI systems for which the keys have been made public, FAST and Bolero. FAST stands for 'First Attempt to Secure Trade'; it is an EU-funded project run by a consortium of Chambers of Commerce. Bolero is also EU-funded, run by a consortium of trading, shipping and telecomms companies, and its purpose is to replace paper bills of lading by electronic documents.

These systems use proprietary formats rather than either X.509 or PGP, so we quote here their root keys' RSA moduli and exponents directly, hex filtered and most significant nybble first. They were introduced to us by the system supplier and thus rate a trust level of 'B':

FAST
c/o F.N.C.C.B
Avenue des Arts 1-2 B.10, B-1040 Bruxelles, Belgium

```
MOD =   FFFFFB33 8C150605 7AAF2290 3D50D23C
        61664505 61A60021 D934ACFD 8EE14EA0
        9728CF00 45EF6C7D D05D2FE2 2700857A
        8EF4399A FE3AED82 77D7FA5E 2F7C5829
EXP =   10001
```

BOLERO
The Bolero User Association
1 Gainsford Street, London SE1 2NE, United Kingdom

```
MOD =   FFFF3FB7 5FFF0DB6 EF0F2516 15DDCDE0
        72DD357F E0DA8C59 4C9683ED 93007C51
        3DECF538 341ECA65 5A7C9C3C 3978557A
        914ADB62 BA204076 47586CB1 9403F99F
EXP =   014321
```

5 Computer Emergency Response Teams

AFCERT
Air Force Information Warfare Center
AFIWC/EACA, 102 Hall Blvd, Ste 215, San Antonio
TX 78243-7013, USA
Tel: +1 210 977 3157
Fax: +1 210 977 3632
afcert@afcert.csap.af.mil
http://afcert.csap.af.mil
B
BB 92 DF 3A : 39 D6 99 3A : : D8 2A 7C 49 : 45 C1 E0 E2 1024

AIX Security
IBM Corporation
11400 Burnet Road, Austin, TX, 78758-3493, USA
Tel: +1 512 838 3459
security-alert@austin.ibm.com
B
78 0A 41 FC : 66 39 3E 3A : : 63 71 7E E1 : AA 90 F9 20 1024

Automated Systems Security Incident Support Team (ASSIST)
Defense Information Systems Agency
ATTN: D334/ASSIST, DISA Headquarters Bldg.
701 South Courthouse Road, Arlington, VA 22204, USA
Tel: +1 800 357 4231
Fax: +1 703 607 4735
assist@assist.mil
http://www.assist.mil
C
08 46 41 49 : CD 4C 44 0D : : D9 FB EF DC : 12 4E 93 E2 1024

AUSCERT
The University of Queensland
Prentice Centre, Brisbane, Queensland, 4072, Australia
Tel: +61 7 3365 4417
Fax: +61 7 3365 7031
auscert@auscert.org.au
http://www.auscert.org.au
B
FA 00 06 3C : D2 B4 B4 DC : : 40 68 73 AC : 31 40 C8 F6 1024

Boeing CERT
The Boeing Company
P.O.Box 3707, Mail Stop 2M-96, Seattle
Washington 98124-2207, USA
Tel: +1 206 657 9353
Fax: +1 206 657 9477
compsec@pss.boeing.com
http://www.boeing.com **B**
1A 2F C6 F0 : 5D E2 5A E0 : : 75 7E 45 3D : 98 F2 00 F3 1024

BSI-CERT
Bundesamt für Sicherheit in der Informationstechnik
Referat V2, Postfach 20 03 63, D-53133 Bonn, Germany
Tel: +49 228 9582 444
Fax: +49 228 9582 427
cert@bsi.de
http://www.cert.dfn.de/eng/csir/europe/bsicert.html **B**
5A 0C 87 59 : 57 65 FE 6A : : 08 39 C6 98 : B8 C1 D0 A9 1024

CARNet CERT
CARNet
c/o SRCE - University Computing Center, Marohniceva ulica bb
10000 Zagreb, Croatia
Tel: +385 1 6164 355
Fax: +385 1 6164 395
c-cert@carnet.hr
http://www.carnet.hr/CCERT/index_eng.html **B**
3C D7 F5 6A : CD DF 24 03 : : 36 A3 E9 18 : 58 EE 4B 32 1024

CERTCC-KR
Korea Information Security Agency
Dong-A Tower 5 fl., 1321-6, Seocho, Seocho, Seoul 137-070, Korea
Tel: +82 2 3488 4119
Fax: +82 2 3488 4129
cert@certcc.or.kr
http://www.certcc.or.kr **D**
B7 1F D8 DE : 74 22 2D 4E : : 0F 92 DD 5E : 24 AE 82 14 1024

CERT Coordination Center
Carnegie Mellon University
4500 Fifth Avenue, Software Engineering Institute,
Carnegie Mellon University, Pittsburgh, Pa 15213-3890, USA
Tel: +1 412 268 7090
Fax: +1 412 268 6989
cert@cert.org
http://www.cert.org **C**
E6 DD E6 E9 : 97 6B 4C FB : : 2E 91 02 68 : DC B4 85 9A 1024

CERT-IT
University of Milan
Dipartimento di Scienze dell'Informazione, Via Comelico 39/41, 20135,
Milano, Italy
Tel: +39 2 55006 300
Fax: +39 2 55006 394
cert-it@security.dsi.unimi.it
http://security.dsi.unimi.it **B**
58 CA 8B 1F : B8 46 A2 4B : : 93 D7 FD 70 : D9 F7 10 9A 1024

CERT-NASK
Krzysztof Silicki
NASK (Research & Academic Network in Poland)
ul.Bartycka 18, 00-716 Warszawa, Poland
Tel: +48 22 8280420
Fax: +48 22 8280420
cert@nask.pl
http://www.nask.pl/NASK/CERT **B**
18 3C 9A AD : E1 25 8B 45 : : 2B 22 2B 9D : AA 06 AA DA 1024

CERT-NL
SURFnet bv
P.O. Box 19035 Utrecht, NL-3501 DA, The Netherlands
Tel: +31 302 305 305
Fax: +31 302 305 329
cert-nl@surfnet.nl
http://www.nic.surfnet.nl/surfnet/security/cert-nl.html **C**
EA 30 C4 F5 : 5E C4 B3 E1 : : DD D6 40 0C : D4 5C E6 19 1024

CERT-Renater
CERT Renater
Tel: +33 1 53 94 20 44
Fax: +33 1 53 94 20 41
certsvp@renater.fr
http://www.urec.fr/Renater/Securite/CERT-RENATER.html **B**
02 1F 9A 79 : A1 80 88 5B : : CD 7A 3E 94 : 71 8B 34 E0 1024

CERT-UU
Academic Computer Centre Utrecht
Attn. CERT-UU, P.O. Box 80011, 3508 TA Utrecht
The Netherlands
Tel: +31 30 253 14 45
Fax: +31 30 253 16 33
cert-uu@ruu.nl
http://www.cs.ruu.nl/cert-uu **C**
5D E5 00 01 : A2 1F A2 E8 : : 1A C7 DB 66 : 28 64 3F 95 1024

Computer Incident Advisory Capability (CIAC)
Computer Security Technology Center
c/o Lawrence Livermore National Laboratory, 7000 East Avenue
Livermore, CA 94550, USA
Tel: +1 510-422-8193
Fax: +1 510-423-8002
ciac@llnl.gov
http://ciac.llnl.gov **B**
3A FC 6B 1F : 0F B2 C2 44 : : 84 81 B6 98 : 03 14 29 3E 1024

DFN-CERT
University of Hamburg
Vogt-Kölln-Straße 30, D-22527 Hamburg, Germany
Tel: +49 40 5494 2262
Fax: +49 40 5494 2241
dfncert@cert.dfn.de
http://www.cert.dfn.de **B**
D7 B0 D1 19 : 19 91 49 B9 : : 47 B5 17 73 : D3 FB A1 77 1024

DK-CERT (UNI-CERT)
Danish CERT
UNI-C, Vermundsgade 5, DK-2100 Copenhagen Ø, Denmark
Tel: +45 35 87 88 89
Fax: +45 35 87 88 90
cert@cert.dk
http://www.cert.dk **D**
81 AF FA DA : 44 BB 3B 87 : : 5B DC 5A CE : 87 CB C6 0E 1024

esCERT-UPC
Universitat Politècnica de Catalunya
c/Jordi Girona, 1-3, Mòdul D6 (Campus Nord)
E-08034 Barcelona, Catalunya, Spain
Tel: +34 3 4015795
Fax: +34 3 4017055
cert@escert.upc.es
http://escert.upc.es

esCERT contact key
21 3C A6 69 : 0C B7 04 AC : : 10 3F 27 A8 : FF 72 7C 76
B 1024

esCERT sign key
B1 CB 0B 4B : 2B C0 DD A8 : : 95 99 B4 86 : 31 91 0A 4A
D 768

EuroCERT
SIRCE
c/o UKERNA, Atlas Centre, Chilton, Didcot
Oxfordshire OX11 0QS, UK
Tel: +44 1235 822 382
Fax: +44 1235 822 398
eurocert@eurocert.net
http://www.eurocert.net
16 A6 55 41 : 25 26 9D D5 : : 3D 32 93 05 : C5 BD C1 54
B 1024

FUNET CERT
Center for Scientific Computing
P.O. Box 405, FIN-02101 Espoo, Finland
Tel: +358 9 457 3210
Fax: +358 9 457 2302
cert@cert.funet.fi
http://www.cert.funet.fi
B3 21 4E 9E : 25 4B 39 6D : : 69 D5 8A 12 : 4C BB CF A0
B 1024

GT-CoC CERT
Georgia Institute of Technology, College of Computing
801 Atlantic Drive Atlanta, GA 30332-0280, USA
Tel: +1 404 894 4736
Fax: +1 404 894 9846
cert@cc.gatech.edu
http://www.cc.gatech.edu
34 3E 0D B5 : 59 61 C6 FE : : 83 C2 57 AC : AB 5A EB 76
B 1024

Hewlett-Packard Company Software Security Response Team
security-alert@hp.com
97 D3 49 C0 : 46 F3 D1 EB : : 94 89 02 C3 : 4C A0 5E DC
C 1024

HUNGARNET-CERT
Nemzeti Információs Infrastruktúra Fejlesztési (NIIF) Program
H-1132 Budapest Victor Hugo 18-22 Hungary
Tel: +36 1 149 79 86
Fax: +36 1 129 78 66
cert@cert.iif.hu
http://www.cert.iif.hu
7F 54 97 16 : F9 28 0B D3 : : AA BE 4B 56 : 39 08 AD 88
B 1024

IBM - Emergency Response Service
IBM Corporation
300 Long Meadow Road, Mail Stop 227, Sterling Forest
NY 10979-0700, USA
Tel: +1 914 759 2901
Fax: +1 914 759 4326
ers-tech@vnet.ibm.com
http://ers.ibm.com **B**
9E 0D 57 58 : 93 FE 8C F7 : : 2A 5C DB 99 : AF 59 46 AC 1024

IRIS-CERT
Centro de Comunicaciones RedIRIS
Serrano, 142, 28006 Madrid, Spain
Tel: +34 1 585 4992
Fax: +34 1 585 5146
cert@rediris.es
http://www.rediris.es/cert **B**
F7 5A A6 6F : D6 25 42 5A : : 48 8C D9 0E : B4 77 3D 75 1024

ISnet CERT
INTIS Inc.
Taeknigardi - Dunhaga 5, 107 Reykjavik, Iceland
Tel: +354 525 4950
Fax: +354 552 8801
cert@cert.isnet.is
http://www.cert.isnet.is **D**
00 F1 37 66 : 52 BD A7 15 : : 9D 10 97 DB : E8 80 8F 3C 1024

JPCERT/CC
Japan Computer Emergency Response Team Coordination Center
Tel: +81 3 5575 7762
Fax: +81 3 5575 7764
info@jpcert.or.jp
http://www.jpcert.or.jp **D**
BA F4 D9 FA : B8 FB F0 73 : : 57 EE 3C 2B : 13 F0 48 B8 1024

MxCERT
ITESM
DINF-DTCI, Suc. de correos “J”, CP 64849, Monterrey, N.L., Mexico
Tel: +528 328 4088
Fax: +528 328 4129
mxcert@mxcert.org.mx
http://www.mxcert.org.mx **B**
B2 F3 6C 2E : 17 CF EC B0 : : 53 89 A7 3B : B9 69 C5 51 1024

NASA Incident Response Team (NASIRC)
National Aeronautics & Space Administration (NASA)
4200 Forbes Blvd. Suite #106, Lanham, MD 20706 USA
Tel: +1 301 918 1970
Fax: +1 301 918 8154
nasirc@nasirc.nasa.gov
http://www-nasirc.nasa.gov **B**
8B FF 41 F0 : F8 0E B6 CE : : 09 70 54 74 : 82 AA CA 10 2048

Naval Computer Incident Response Team (NAVCIRT)
US Navy
Tel: +1 757 417 4024
Fax: +1 757 417 4010
navcirt@fiwc.navy.mil
http://infosec.nosc.mil **D**
CF 22 86 6D : 77 64 3B B5 : : A5 82 CD 33 : 4F 4D BC 49 1024

NORDUnet CERT
NORDUnet A/S
Agern Allé 3, DK-2970 Hørsholm, Denmark
Tel: +45 45 76 23 00
Fax: +45 45 76 57 08
cert@nordu.net
http://www.nordu.net/cert **B**
E2 D5 58 D0 : 53 A9 F4 4C : : B6 3A 6F DC : 2F 86 AC A9 1024

OxCERT
University of Oxford
OUCS, 13 Banbury Road, Oxford OX2 6NN, UK
Tel: +44 1865 282222
Fax: +44 1865 273275
oxcert@ox.ac.uk
http://info.ox.ac.uk/compsecurity/oxcert **B**
1B 5B 6D 79 : F2 35 49 3C : : 27 38 FC 09 : 45 26 65 BD 1024

PCERT
Eugene Spafford
Purdue University
pcert-request@cs.purdue.edu
http://www.cs.purdue.edu/pcert **B**
9F 30 B7 C5 : 8B 52 35 8A : : 42 4B 73 EE : 55 EE C5 41 1024

SARA-CERT
Stichting Academisch Rekencentrum Amsterdam
Kruislaan 415, 1098 SJ Amsterdam, The Netherlands
Tel: +31 20 592 3000
Fax: +31 20 668 3167
cert-sara@sara.nl
http://www.sara.nl **D**
72 2E 70 8A : 8A 7E 48 68 : : 33 39 7B B1 : 3F 16 72 1B 1024

Security Emergency Reaction Center (SERC)
Science Applications International Corporation (SAIC)
serc@serc.saic.com **B**
FA 20 D0 3B : 54 DE 29 7B : : 60 ED 7E DC : 43 0E 63 D0 1024

SGI Customer Security Coordinator
Silicon Graphics Inc.
2011 N. Shoreline Blvd., Mountain View, CA 94043, USA
agent99@csd.sgi.com
http://www.dcrt.nih.gov/security/dcrtcert.html **B**
5E 93 70 33 : 24 05 6C 5B : : A0 3C 89 21 : 3F 0F 48 56 1024

SNI-CERT
Siemens-Nixdorf AG
SNI OEC HES XP2 D-81730 Muenchen, Germany
Tel: +49 89 636 52885
Fax: +49 89 636 44887
sni-cert@mch.sni.de
http://www.sni.de **B**
EA 07 C5 0F : E6 C7 25 4B : : 2F 9F 87 D5 : D1 5C A6 06 1024

Slovenian CERT (SI-CERT)
ARNES SI-CERT
Jamova 39, 1000 Ljubljana, Slovenia
Tel: +386 61 125 1515
Fax: +386 61 125 5454
si-cert@arnes.si
http://www.arnes.si/si-cert **B**
BA A5 2F CF : 0F 5D A1 F2 : : 4A 23 B7 33 : 98 32 BB F6 1024

SUNET CERT
Swedish University Network
cert@sunet.se
http://www.sunet.se **D**
04 9C D7 DA : 9F 18 8F 73 : : E2 01 82 43 : 1E 2A DE AF 1024

SWITCH-CERT
The Swiss Academic and Research Network
Limmatquai 138, CH-8001 Zurich, Switzerland
Tel: +41 1 268 1518
Fax: +41 1 268 1568
cert-staff@switch.ch
http://www.switch.ch/switch/cert

SWITCH-CERT-1998-Key **C**
28 BF 57 B1 : DC CC 84 8E : : 23 36 A2 37 : AF 18 2D 10 1024

SWITCH-CERT-1997-Key **B**
DC 44 49 C5 : 09 EB D8 C0 : : B2 CE 7D 26 : 46 6D 24 9E 1024

SWITCH-CERT-1996-Key **B**
DE 6F 14 91 : 65 6B AF 45 : : 65 2C 49 AD : 17 85 39 E1 1024

UNI-Cert
Unisource NL bv
P.O. Box 90934, NL - 2509 LX, The Hague, The Netherlands
Tel: +31 703 818 606
Fax: +31 703 819 615
uni-cert@cert.unisource.nl
http://www.cert.unisource.nl **B**
AF 96 A0 77 : 8A 4E 72 00 : : 56 90 60 32 : 6B EE 48 46 1024

Uninett CERT/SIKT
Uninett
Postbox 6883, Elgeseter, N-7002 Trondheim, Norway
Tel: +47 73 59 29 80
Fax: +47 73 59 64 50
cert@uninett.no
http://www.uninett.no/info/cert **D**
E1 42 21 2D : 00 0C B3 6C : : 8D E2 44 71 : 7D 83 CD EA 1024

6 Other Institutional Keys

ALWIL Software
Pavel Baudis
Lipi 1244, 193 00 Prague 9, Czech Republic
Tel: +420 2 81 92 16 61
Fax: +420 2 81 92 16 64
baudis@asw.cz
http://www.anet.cz/alwil/alwil.htm

A 1024

A4 3D D1 40 : D2 92 EB 1A : : E5 FB 64 A1 : 70 00 AA 71

CompuServe Internet Security
George Jones
5000 Britton Rd., PO BOX 5000, Hilliard, Ohio 43026-5000 USA
Tel: +1 614 723 4560
Fax: +1 614 723 1221
security@compuserve.net

C 1024

64 4B C2 85 : 09 A4 49 4A : : 08 80 7E 79 : 9E 3E 05 7F

c't Magazine Certificate
Erich Kramer
Verlag Heinz Heise GmbH & Co KG
Helstorfer Str. 7, D-30625 Hannover, Germany
pgpCA@ct.heise.de
http://www.ct.heise.de/ct/

A 1024

22 09 55 9D : 72 60 87 B0 : : 02 C3 71 9C : 4E 0E 07 77

DFN-PCA, Certification Key Only (Low-Level: 1997-1998)
Stefan Kelm and Britta Liedkte

B 2048

09 7C 09 19 : D3 C3 86 DC : : 7A 30 15 11 : 12 95 8D E3

Doctors-Web.com, Certification only key
Frank A. Friedrichs
Germany
cert-info@doctors-web.com

C 2048

BB 90 59 AF : 91 6D 1D 70 : : C9 7E D2 E4 : 0F 04 F0 C6

Entropia Internet Notary Service
1038 Corvette Drive, San Jose, California 95129-2903 USA
Tel: +1 408 255 2388
entropy@entropia.com
http://entropia.com/notary/

C 2047

55 FD 14 61 : 70 34 4D 14 : : EE 3C 98 EE : 8D E9 29 B3

German Keyserver Master Certification Key
Christian Kanja
Glueck & Kanja GmbH
Bernardstraße 112, D-63067 Offenbach, Germany
Tel: +49 69 800706 220
Fax: +49 69 800706 66
pgpCA@keyserver.de
http://www.keyserver.de
DC 95 F7 8C : 0D 32 4D 82 : : 07 A9 97 3A : F0 3B F1 EA — **C** 2048

Gesellschaft zur Förderung kommunikativer Medien e.V.
GeFökoM CA
Manuel Thierschmidt
Schadewitzststraße 22, D-97074 Würzburg,Germany
Tel: +49 931 79 00 20 0
Fax: +49 931 78 12 62
certificate@mayn.de
http://www.mayn.de/ca/
56 C2 13 CA : B8 3C BA 46 : : 57 2E 34 75 : ED F0 FF F7 — **C** 2048

Glueck & Kanja Corporate Certification Key
Christian Kanja
Glueck & Kanja GmbH
Bernardstraße 112, D-63067 Offenbach, Germany
Tel: +49 69 800706 220
Fax: +49 69 800706 66
pgpCA@glueckkanja.de
http://www.glueckkanja.de
2F F2 2D 90 : DE C6 7F 11 : : 30 EE 98 82 : AA E0 08 EE — **C** 2048

Highware, Inc.
info@highware.com
support@highware.com
A6 BA 12 BE : AC FB 03 8E : : 5A A5 38 85 : E8 17 03 37 — **C** 1024

Individual Network e.V. Root-CA
Lutz Donnerhacke or Ingmar Camphausen
in-ca@individual.net
https://www.in-ca.individual.net/
B3 06 9A 8D : 38 04 3C 75 : : 41 32 EE DC : 8B 7D 61 0D — **A** 2048

I.T. Consultancy Limited Timestamp Service
Jersey, Channel Islands, British Isles
stamper@itconsult.co.uk
http://www.itconsult.co.uk/stamper.htm
4B 12 BC D5 : 78 85 11 06 : : 3B 54 31 90 : E0 9D F3 06 — **C** 2046

Loughborough University Public Key Accreditors
Martin Hamilton
Computing Services, Loughborough University
Leics. LE11 3TU, United Kingdom
pgp-keys@lboro.ac.uk
http://www.lboro.ac.uk/computing/
FF BA B8 66 : 18 D2 89 7A : : F4 03 C9 D1 : 42 2F F2 2C — **C** 1024

R-Cube Systems Ltd Key Certification
Paul Rouse
R-cube Systems Ltd
2-4 Henry Street, Bath, BA1 1JT, United Kingdom
certs@r-cube.co.uk
http://www.r-cube.co.uk/
1A CC F6 56 : EF A8 F2 66 : : 67 27 04 05 : FC 20 AB 9D — **C** 1024

RRZE Security Administration
University of Erlangen-Nürnberg - RRZE (Computer Centre)
Martensstraße 1, 91058 Erlangen, Germany
secadm@rrze.uni-erlangen.de
http://www.rrze.uni-erlangen.de/RRZE/
8A 63 C6 C0 : D6 4E AF 4A : : 0C 1D 65 7A : E5 33 DB B5 — **C** 1024

Sandelman Software Works Corporation
Michael C. Richardson
152 Rochester Street, Ottawa, ON, K1R 7M4 Canada
root@sandelman.ottawa.on.ca
http://www.sandelman.ottawa.on.ca/
74 E3 C3 72 : EA EB 72 B8 : : 03 3D 68 AB : D3 5C 4F 42 — **C** 1024

SkyNet, a.s. - CZ TIS Authorized Security Partner
Roman Pavlik
Kabatnikova 5, 602 00 Brno, Czech Republic (until May 1, 1998)
Ptasinskeho 6, 602 00 Brno, Czech Republic (after May 1, 1998)
Tel: +420 5 41 24 59 79
Fax: +420 5 41 24 59 82
Roman.Pavlik@SkyNet.cz
http://www.SkyNet.cz
F8 E5 48 D1 : 46 95 4F EB : : 1F 15 A9 29 : AF BE C4 A5 — **A** 1024

UK Academic PCA
Ian Brown
Department of Computer Science, University College London
Gower Street, London WC1E 6BT, United Kingdom
Tel: +44 171 419 3716
Fax: +44 171 387 1397
pgp-pca@cs.ucl.ac.uk
http://www.cs.ucl.ac.uk/staff/I.Brown/ca/ **A**
18 CA E2 5E : C4 F3 7D 3F : : 43 4B 14 0B : 44 EF 3B 9E 1024

University of Cambridge, Computer Laboratory
Computer Laboratory, University of Cambridge
Piete Brooks
Pembroke Street, Cambridge CB2 3QG, United Kingdom
Tel: +44 1223 334600
Fax: +44 1223 334678
http://www.cl.cam.ac.uk/DeptInfo/pgp-keys.html

Accreditor 1
pgp-keys1@cl.cam.ac.uk **A**
15 FA B5 33 : F4 63 92 D7 : : C2 47 29 8B : A1 D9 7D C0 1024

Accreditor 2
pgp-keys2@cl.cam.ac.uk **A**
79 BC 12 87 : 64 52 88 73 : : 3E 4D B3 C4 : 54 0F A0 49 1024

Accreditor 4
pgp-keys4@cl.cam.ac.uk **A**
3F E8 62 D6 : E7 EE D8 2B : : 4A 91 58 DC : D2 4C A8 0A 1024

University of Manchester and UMIST PGP Key Certification
pgp@man.ac.uk, pgp@umist.ac.uk, pgp@mcc.ac.uk **C**
E8 84 2D 07 : 07 EF A9 6F : : 7F BA E1 0A : ED 22 67 F6 2048

7 Personal Keys

In this section we include a number of personal PGP keys followed by the personal keys of some Entrust/Solo users.

PGP Keys

Jérôme Abela
10 place du Theatre, 92310 Sèvres, France
Jerome.Abela@efrei.fr
37 B8 44 0A : C2 8C 77 40 : : BB 98 CB D2 : B2 B9 32 C3
B
1024

Tomas Ahl
pbn@lysator.liu.se
http://www.lysator.liu.se/~pbn/
17 79 EC 05 : AF 81 D6 5F : : A0 0D C5 DF : E7 E8 C9 88
C
1024

Osma "Tau" Ahvenlampi
oa@iki.fi
34 C0 CE C1 : 41 17 C5 2A : : 2B 99 14 1E : 6C 4C 9A BF
C
1536

Leslie L. Aker, Sr.
aker@itd.nrl.navy.mil
A8 C7 0E 86 : 1D 78 2A FB : : 49 BC 24 88 : 2E FF 6A AB
C
1024

Wichert Theodorus Akkerman
Debian GNU/Linux, Leiden University
wakkerma@debian.org, wakkerma@wi.leidenuniv.nl
http://www.wi.leidenuniv.nl/~wichert/
38 44 4C 2C : A6 AD 75 6E : : B4 A2 E5 FA : 61 2A FF 59
C
768

Tom Almy
almy@teleport.com
1:105/290@fidonet.org
http://www.teleport.com/~almy/
25 4A EB 71 : 55 62 F4 7F : : 41 C0 4D B7 : 59 2A E1 81
C
1024

Alan Amesbury
University of Minnesota, IT Systems Staff
amesbury@itlabs.umn.edu
http://www.cs.umn.edu/~amesbury
0E E0 6C B7 : 7F D0 3C CA : : EE B9 B4 0C : BB 13 51 1B
C
2048

Paul Anderson
LDCS, Department of Computer Science, University of Edinburgh
Edinburgh EH9 3JZ, United Kingdom
Tel: +44 1316 505193
Fax: +44 1316 677209
paul@dcs.ed.ac.uk
http://www.dcs.ed.ac.uk/~paul/

C 512

A3 31 BC FD : 70 FE 9D 3E : : 18 CC 36 AB : 56 F6 CB C8

Ross J. Anderson
University of Cambridge, Computer Laboratory
Pembroke Street, Cambridge CB2 3QG, United Kingdom
Tel: +44 1223 334733
Fax: +44 1223 334678
Ross.Anderson@cl.cam.ac.uk
http://www.cl.cam.ac.uk/~rja14

A 1024

E5 C7 93 BE : 37 9D 28 42 : : 49 DC A8 09 : A1 47 05 F6

Andreas M. Antonopoulos
andreas@droopy.demon.co.uk

C 2048

4A CF 27 F9 : 18 1C BD C3 : : 2C 7D EE B9 : CC F7 E2 6B

Heinz-Ado Arnolds
IFNS GmbH
Max-Planck-Straße 37, D-50858 Köln, Germany
arnolds@ifns.de

C 1024

6F 88 75 56 : 6C 29 7A 82 : : 91 F8 EC 7C : 0C C0 07 84

Hannu Aronsson
Kuusitie 9A29, 00270 Helsinki, Finland
haa@cs.hut.fi
http://iki.fi/haa/

C 1024

7F 5F 69 1B : C5 AD FD 89 : : 34 F0 67 AE : A2 5B BD 26

Pål Axelsson
Uppsala university
Box 887, S-751 08 UPPSALA, Sweden
Tel: +46 18 4717918
Fax: +46 18 4717725
Pal.Axelsson@its.uu.se

C 1024

37 5D AF 0B : 2C A7 31 FE : : 2C 7C 57 6E : C8 1D D4 0E

Jason R. Baker
jbaker@themis.ag.gov.bc.ca

C 1024

36 31 1C 85 : 23 8E CE AF : : 35 9D BD 39 : 4E 76 11 1D

Stan Barber
sob@academ.com
C
92 2E 1D AF : 8C F0 0B 21 : : B2 4B 05 1A : 6F DD F2 0B 1024

David Barr
Department of Computer and Information Science
Ohio State University
395 Dreese Labs, 2015 Neil Avenue, Columbus, OH 43210, USA
barr@cis.ohio-state.edu
http://www.cis.ohio-state.edu/~barr/
C
B7 D9 13 C7 : E4 C6 D9 1B : : 7B 32 D3 E6 : F2 B9 21 25 1024

Robert Baskerville
Langdale Hall, Upper Park Road, Victoria Park, Manchester M14 5RJ
Robert@Baskerville.Net
http://www.baskerville.net/
C
51 F6 BD 6F : F2 E5 E4 68 : : 91 FD F8 A0 : CC D8 AC C0 1024

Matthias Bauer
IMMD 1
Unversität Erlangen-Nürnberg
Martensstraße 3, 91058 Erlangen, Germany
matthiasb@acm.org
C
45 C9 94 9D : 34 62 E5 4A : : A2 6E F9 AF : AF AE 63 7F 1024

Michael Baumann
Optivus Technology Inc., Loma Linda University Medical Center
San Bernardino, California, USA
Tel: +1 909 799 8308
baumann@llumc.edu
C
7B 2F A4 D5 : FA B3 B5 5E : : 4D DA E0 85 : 7A DD C3 76 1024

Michael Baumer
Verein der Informatikstudierenden an der ETH Zuerich
baumi@vis.inf.ethz.ch
C
A8 E3 D9 73 : 72 8F E2 60 : : 87 BC 86 4B : 53 86 B5 79 2048

Bill Bauriedel
Stanford University
Polya Hall Room 215, M/S 4136, Stanford University
Stanford, CA 94305, USA
Bill.Bauriedel@Forsythe.Stanford.edu
http://www-leland.stanford.edu/~billb
C
9C 70 59 A0 : 99 2F A4 4D : : 9D C4 F6 A9 : CB 48 7E 1D 1024

Mark D. Baushke
mdb@cisco.com
68 64 91 83 : 97 48 B6 2B : : DB 87 54 01 : FE 1F 27 67
C
1024

Wolfgang Behn
be@paul.ping.de
D4 10 93 C7 : EC 2B A1 1D : : B2 FC 71 06 : 7D 63 5B 5B
C
1024

Bodo Bellut
Klosterstraße 7, Dortmund 44135, Germany
Tel: +49 231 5860337
bodo@garfield.ping.de
AE 5A 47 40 : 5A A0 D6 15 : : 8E 54 44 AA : 8D DD 6E BD
C
768

Bill Bereza
bereza@pobox.com
http://www.pobox.com/~bereza/
07 0C EB 83 : 57 6E 14 58 : : A3 37 4D 99 : 87 94 C9 53
C
1024

Francesco Bergadano
Dipartimento di Informatica, Università di Torino
Corso Svizzera 185, 10149 Torino, Italy
Tel: +39 11 7429243
Fax: +39 11 751603
bergadan@di.unito.it
http://maga.di.unito.it/fb
F0 00 2A D7 : 01 F9 4C 7C : : F5 61 43 FF : F2 9A C7 A0
A
1024

Magnus Bergroth
Mälardalens Högskola, Box 883, S-721 23 Västerå, Sweden
Tel: +46 21 101583
Fax: +46 21 101440
magnus.bergroth@mdh.se
B6 ED 0C 6B : 8D 09 4A 0E : : AA C0 18 57 : 83 6B 06 AF
C
1024

Vincent Berkhout
Vincent.Berkhout@DANTE.org.uk
E2 57 CB 6C : 26 AD 5A CE : : 48 C0 F9 CF : 90 59 96 E2
C
1024

Jochen P. Bern
FB IV - Informatik
Universität Trier, 54286 Trier, Germany
bern@itwm-trier.fhg.de
http://www.informatik.uni-trier.de/~bern/
86 84 A8 BF : E4 85 3F 85 : : 71 23 FB 8A : AF 86 EF E6
C
1024

Patrick Bernier
6251, 8th avenue, Montréal, Québec, H1Y 2M3 Canada
pat@4p.com
http://www.mlink.net/~bernier/
31 3C 0B BB : 44 BF CE B1 : : 69 1E 84 53 : 83 CB B4 2B
C
1024

Kevin Berry
spamite@iname.com
http://www.chrysalis.org/kevinb
CD E4 09 61 : 52 DF BB 9C : : 61 92 AC E4 : 29 0C FC 04
C
2047

Johann Bezuidenhoudt
PO Box 2023, Northcliff 2115, South Africa
johann@aztec.co.za
FD AB C2 78 : EF AB 06 E2 : : BE B8 A0 A7 : E7 B9 40 F2
A
2047

Marc Blanchet
Marc.Blanchet@viagenie.qc.ca
57 86 A6 83 : D3 A8 58 32 : : F7 0A BB BD : 5F B2 4B A7
C
1024

Matt Bishop
Department of Computer Science, University of California
Davis, CA 95616-8562, USA
bishop@cs.ucdavis.edu
http://seclab.cs.ucdavis.edu/~bishop/
29 C9 63 9D : 22 F3 5A 7B : : 2A FA D4 EA : 7A 04 D4 FE
C
1024

Johannes H. Blaschy
TMS GmbH
Laubaner Straße 12, 31139 Hildesheim, Germany
Tel: +49 5121 2907 0
Fax: +49 5121 2907 25
Johannes.Blaschy@iname.com
DE 6B 5D 35 : A4 A1 35 10 : : E6 9E 13 F0 : 50 C3 74 CC
C
2048

Mason Loring Bliss
34 Beach street, Middleborough, MA 02346-3718, USA
mason@acheron.middleboro.ma.us
http://www.webtrek.com/mason
35 82 7C 5A : C6 9B F6 F3 : : 76 EA 4A 18 : 46 0D 21 0B
C
1024

Chris Blum
CIP-Pool der Philosophischen Fakultaet, Universitaet des Saarlandes
Im Stadtwald, Geb. 44, D-66041 Saarbruecken, Germany
chris@phil.uni-sb.de
1F A0 65 A7 : 6C AF 9D CA : : E4 96 2A 8F : 90 09 29 A9
C
1024

Sarr Blumson
ITD, University of Michigan
535 W William, Ann Arbor, MI 48103-4943, USA
Tel: +1 313 764 0253
Fax: +1 313 763 8937
sarr@citi.umich.edu
http://www-personal.umich.edu/~sarr/

C 512

```
89 0B 6C AD : CE D8 A9 3C : : 1B 30 06 3E : 0E DB BC 14
```

Andreas Bogk
andreas@ccc.de

C 1024

```
4F 58 91 38 : 16 05 3B A1 : : 8B D9 38 3B : E4 20 D3 89
```

Vesselin Vladimirov Bontchev
Postholf 7180, IS-127, Reykjavik, Iceland
Tel: +354 561 7273
Fax: +354 561 7274
bontchev@complex.is

B 1024

```
E5 FB 30 0C : D4 AA AB 44 : : E5 F7 C3 18 : EA 2B AE 4E
```

Nathaniel Borenstein
First Virtual Holdings
nsb@fv.com

C 1024

```
D3 78 9F 33 : 68 C1 24 D5 : : 7A ED D0 DC : 85 9E 8C 02
```

Caspar Bowden
Scientists for Labour
41 Great Percy Street, London WC1X 9RA
cb@qualia.co.uk

A 2001

```
5F 4D BF 0B : 55 93 95 7B : : 37 5C DE A5 : 66 1B 82 ED
```

Richard Peirce Brent
Oxford University Computing Laboratory
Wolfson Building, Parks Road, Oxford, OX1 3QD, England
Tel: +44 1865 283504
Fax: +44 1865 273839
Richard.Brent@anu.edu.au
http://discus.anu.edu.au/~rpb/

C 1024

```
E3 BD 31 11 : CF 80 5E 82 : : D8 9E F1 A4 : B7 F7 F7 F1
```

David Bridgham
dab@froghouse.org

C 1024

```
BE 0C B7 71 : 77 10 14 21 : : AD D8 77 62 : 10 D9 CC 69
```

Lawrie Brown
Lawrie.Brown@adfa.oz.au

C 750

```
7E 2E F1 10 : 3C 04 8A 79 : : 51 F2 17 A0 : B8 5F 28 C1
```

Barry L. Brumitt
belboz@frc2.frc.ri.cmu.edu
E2 DD EC C1 : D8 10 FC 81 : : B3 CC 98 F8 : 8F 53 1F EE
C 1024

Jordi Buch
Universitat Politècnica de Catalunya
Mòdul D6, 08034 Barcelona, Spain
jbt@sirius.ac.upc.es
http://sirius.ac.upc.es/~jbt/
CD 80 43 D4 : C8 3E 1A C8 : : E3 18 B7 B1 : EA F4 F5 0C
C 768

Matthias K. Buelow
Bruesseler Straße 3, D-97084 Wuerzburg, Germany
token@altair.mayn.de
http://luzifer.mayn.de/token/
B2 88 42 1D : BC 7A F6 4D : : FB F5 1D F4 : 57 84 3B 70
C 1024

Thomas Büschgens
sledge@rw.sni.de
8D 85 13 4B : D9 32 DF 7A : : 53 D4 62 BB : 08 8E 54 63
C 1024

John Bull
APM Ltd
Poseidon House, Castle Park
Cambridge CB3 0RD, United Kingdom
Tel: +44 1223 568941
Fax: +44 1223 359779
John.Bull@ansa.co.uk
95 5F F4 A4 : 1D 57 3B 1D : : 4C 35 3A 9B : 81 12 EB C5
C 1024

Willi Burmeister
Department of Computer Science, Kiel University
Preusserstraße 1-9, D 24105 Kiel, Germany
Tel: +49 431 5604 98
Fax: +49 431 5661 43
wib@cs.uni-kiel.de
http://www.informatik.uni-kiel.de/~wib/
51 71 2E AF : A3 25 A1 10 : : 1F 91 97 87 : FD F1 AD D7
C 1024

Ingmar Camphausen
Berlin, Germany
ingmar@in-berlin.de
97 B8 54 ED : 69 4A E4 D1 : : BC 9E F4 C4 : A1 95 F9 9A
C 1024

Bjorn Carlsson
bc@ebone.net
AF E8 5A 80 : 37 F0 C4 BB : : E8 BB 5A 57 : 50 61 20 DA
C 1024

Jeffrey James Bryan Carpenter
P.O. Box 471, Glenshaw, PA 15116-0471, USA
Tel: +1 412 486 6198
Fax: +1 412 486 6376
jjc@pobox.com
http://pobox.com/~jjc/

C 1024

60 17 00 B0 : 9A D8 3B D5 : : 3E A7 36 B6 : 68 0C 1D 96

Shaw Chuang
University of Cambridge, Computer Laboratory
Pembroke Street, Cambridge CB2 3QG, United Kingdom
Fax: +44 1223 334678
Shaw.Chuang@cl.cam.ac.uk

A 1024

8F B1 D4 5C : 17 6E 9F D5 : : 1D 78 90 61 : EB 18 81 49

Peter Conrad
Opus 5 Interaktive Medien GmbH
Friedhofstraße 72, 63263 Neu-Isenburg, Germany
Tel: +49 6102 7761 0
Fax: +49 6102 7761 50
conrad@unix-ag.uni-kl.de
http://www.unix-ag.uni-kl.de/~conrad

C 1024

F7 49 4E A3 : C6 8F 89 0B : : E7 73 34 32 : 0B 29 83 81

Ian C. Cook
ian.cook@citicorp.com

C 1024

8B 0B 67 90 : B5 55 CB D8 : : D7 19 33 09 : CA 72 B6 6B

Lance M. Cottrell
Infonex Internet Inc. & Anonymizer Inc.
loki@obscura.com
http://www.obscura.com/~loki

C 2048

24 5E 55 28 : C4 E3 94 32 : : D3 8E 8F CB : 4C F9 4F 2E

John F. Courtney
PacifiCare Health Systems
courtney@jordi.phs.com

C 1024

2E C2 9E 3D : 8B 71 F2 E9 : : 90 54 30 8D : 18 03 CC 77

Yanik Crépeau
53 Chemin Drayton, Pointe-Claire QC, H9S 4V4 Canada
Tel: +1 514 992 2864
Fax: +1 514 992 3006
yanik@mlink.net, yanik@planon.qc.ca
http://www.mlink.net/~yanik/

C 512

7D 24 DD 59 : C0 FD 73 80 : : 37 40 52 E2 : 1C 5F 1C BC

Frank D. Cringle
Heidestraße 52, 58239 Schmerte, Germany
Tel: +49 2304 467101
Fax: +49 2304 943357
fdc@cliwe.ping.de
http://www.ping.de/~fdc
C 1024
AD 8A 2B D3 : 39 10 73 63 : : 6B 8B 58 1B : 1D 99 CC EF

Bruno Crispo
University of Cambridge, Computer Laboratory
Pembroke Street, Cambridge CB2 3QG, United Kingdom
Tel: +44 1223 334719
Fax: +44 1223 334678
Bruno.Crispo@cl.cam.ac.uk
http://www.cl.cam.ac.uk/~bc201
A 1024
1A D1 4A 1C : EE DD 32 D9 : : EC 5F 0C 93 : 17 C1 C6 5D

Bob Cunningham
bob@lava.net
C 1024
A3 FB 8C 13 : 7A D5 EC 61 : : 7F 99 7D CA : 99 AB 5A 3A

J.H.M. Dassen (Ray)
Department of Computer Science, Leiden University
P.O. Box 9512, 2300 RA Leiden, The Netherlands
jdassen@wi.LeidenUniv.nl
http://www.wi.LeidenUniv.nl/~jdassen/
C 1024
DD 60 32 60 : F7 90 64 80 : : E7 6F D4 E4 : F8 C9 4A 58

Christopher Davis
ckd@kei.com
B 1024
46 8E FD F5 : 12 8E 13 4C : : 2C 8A 92 A3 : B0 D5 2A 5E

Butch Deal
butch@keep.blackmagic.com
C 768
2B AB 70 E7 : C9 4A C8 15 : : 24 AD 74 8B : 4D A4 73 56

Richard Deal
rdeal@atl.lmco.com
C 768
7F 48 05 5F : A3 3F F4 5B : : D7 4C 58 0A : 3E 0A D7 9B

Holger Denz
holger.denz@www.jura.uni-tuebingen.de
http://www.jura.uni-tuebingen.de/~zxmdz01/
C 2048
F5 68 06 71 : B1 F3 51 E9 : : DC FC 73 7B : 89 55 9D 62

David DeSimone
fox@metronet.com
http://www.metronet.com/~fox/
5B 47 34 9F : 3B 9A B0 0D : : AB A6 15 F1 : BB BE 8C 44
C
768

Robert Jon Diamond
Sun Microsystems
Somerset, NJ, USA
rob.diamond@east.sun.com
http://www.well.com/user/diamond
D1 13 BA 49 : AF 7A A5 17 : : 81 99 2F 6E : 6F 28 BE 4C
C
768

Barbara L. Dijker
Labyrinth Computer Services
PO Box 4626, Boulder CO 80306, USA
Tel: +1 303 589 2327
Fax: +1 303 443 9718
barb.dijker@labyrinth.com
03 3D 48 EE : B2 38 F8 04 : : D8 10 8F 4A : B4 E1 CB 89
C
768

Christian Dirks
glasstiger@ocean.gun.de
2F FA B4 69 : 30 97 36 6E : : DC 09 71 28 : 03 5A CD 48
C
2048

Gert Doering
Dewetstraße 18, 80807 München, Germany
Fax: +49 89 35655025
gert@greenie.muc.de
http://www.muc.de/~gert/
CB 1A 7F 91 : 8B 42 C1 0E : : 0B 5F 57 ED : 05 0B DD E8
C
1024

Bryn Robert Dole
dole@incog.com
F1 55 73 E5 : 11 55 1C A0 : : C6 BB 07 7C : 66 A9 2D 0E
C
1024

Lutz Donnerhacke
Lutz.Donnerhacke@jena.thur.de
A4 C1 50 8F : 00 D9 28 60 : : 70 BB 0B 5D : D9 3A 0B B6
A
2048

John Dovey
18 Cecilia Street, Paarl, 7646, South Africa
Tel: +27 21 8084100
Fax: +27 21 8084336
pjcd@bib.sun.ac.za
http://www.sun.ac.za/local/library/john/
E9 5B 15 9F : D9 0C 63 4F : : 59 A5 34 D4 : 2D 86 09 1D
C
1024

Achim Dreyer
adreyer@math.uni-paderborn.de
E9 92 EC 4A : E4 90 8F C0 : : 53 D1 F9 D7 : 56 7F CB 3C
C
1024

Philip L. Dubois
dubois@csn.org
9C DC D8 1D : 93 BA 1E CB : : 6C B4 01 A5 : 4E 1E AE 8F
B
1024

Mario Dueck
m.dueck@3landbox.comlink.apc.org
50 BE 4C 00 : FE 74 18 6C : : 3D 44 18 E6 : D7 F1 A0 6C
C
512

Andreas Dworsky
dworsky@rrz.uni-koeln.de
E1 26 0B 85 : 38 DC 34 BD : : 9A DD 46 C7 : 95 8D E5 95
C
2048

Mirko Dziadzka
dziadzka@fh-furtwangen.de
http://www.ai-lab.fh-furtwangen.de/~dziadzka/
68 72 47 A7 : 4E 71 25 F0 : : 56 02 2D 06 : 58 52 7D AD
D
1024

Lars Eilebrecht
German Unix-AG Association
Glück-Auf-Straße 23, 57223 Kreuztal, Germany
Tel: +49 2732 591701
Fax: +49 2732 591702
sfx@unix-ag.org
http://www.si.unix-ag.org/~sfx/
7B 8A E3 E0 : 8C 63 04 57 : : 77 72 39 E6 : 5A 7E 51 FC
C
999

Carl M. Ellison
207 Grindall Street, Baltimore MD 21230, USA
Tel: +1 410 727 4288
cme@cybercash.com
http://www.clark.net/pub/cme
61 E2 DE 7F : CB 9D 79 84 : : E9 C8 04 8B : A6 32 21 A2
A
1024

Martin Emmerich
München, Germany
me@grmbl.muc.de
http://www.muc.de/~me
B3 B2 5D E8 : 9B 6F BF 57 : : B3 88 3C 1A : 78 57 3A 60
C
1024

Kent Engström
kent@lysator.liu.se
http://www.lysator.liu.se/~kent/
06 E3 14 99 : 2E 4B 4D B3 : : D4 56 DD 55 : F8 FD D5 65
C
1024

Era Eriksson
Idrottsvägen 22 a 23
Fin-01370 Vanda, Finland
era@iki.fi
http://www.iki.fi/~era/
85 40 A8 84 : 71 26 2C ED : : 15 CF 22 82 : 91 01 D4 42
C
768

Leif Erlingsson
Data Lege
Glavagatan 33, 123 71 Farsta, Sweden
Tel: +46 8 604 0995
Fax: +46 8 605 2551
leif@lege.com
http://www.lege.com
DB 47 2F B1 : F8 6B E5 92 : : 7A 97 5C C8 : 7E 62 CA 7C
C
1024

Jon Fairbairn
18 Kimberley Road, Cambridge CB4 1HH, United Kingdom
Jon.Fairbairn@cl.cam.ac.uk
B7 43 07 ED : 3C 76 E5 FD : : 0A 3B 17 F3 : 74 9D DC DD
C
1024

Edward A. Falk
falk@despams.r.us.com
7D CE 1F 28 : 30 B8 17 CB : : E4 6C 1B FC : 71 03 C7 60
C
512

Patrick D. Farrell
pfarrell@cybercash.com
50 FA 4A 83 : 56 CD 8B B2 : : 26 70 3D BB : 64 94 3B 0A
C
1024

Patrick Feisthammel
Winterthurerstraße 43, CH-8004 Uster, Switzerland
Tel: +41 1 994 4035
Fax: +41 1 994 4036
pafei@rubin.ch
http://www.rubin.ch/pafei/
AD 23 A1 90 : B1 2B AF BA : : 44 49 16 7E : 3D A0 F3 C3
C
2020

Lars Fenneberg
Böttgerstraße 29, 22851 Norderstedt, Germany
lf@elemental.net
http://www.elemental.net/~lf/
D1 28 F1 FF : 3C 6B C0 27 : : CC 9C 6C 09 : 34 0A 55 18
C
1024

Kai Fett
Muenzstraße 8, 42281 Wuppertal, Germany
kfett@kfett.wupper.de
http://www.schnism.net
C
53 7C 34 F9 : 0E 48 7B 02 : : 3E B6 FD 50 : 91 8C A1 E1
768

Bettina Fink
c/o Kirchwitz, Seesener Straße 69, 10709 Berlin, Germany
laura@krell.snafu.de
C
E5 82 7E 4C : 08 1A A4 F6 : : DD 63 82 F8 : AF D7 31 C3
1024

Bernd Finkbein
Technische Universität München
Arcisstraße21, D-80333 München, Germany
Tel: +49 89 289 23678
Fax: +49 89 289 63678
Finkbein@e-technik.tu-muenchen.de
http://www.regent.e-technik.tu-muenchen.de/~bef
C
E6 EC AD 89 : D3 17 0A 86 : : 6A 70 AD 33 : 3A C7 4F A3
1024

Jon Finke
Server Support Services
Rensselaer Polytechnic Institute, 1108 th Street, Troy, NY 12180, USA
Tel: +1 518 276 8185
Fax: +1 518 276 2809
finkej@rpi.edu
http://www.rpi.edu/~finkej
C
06 4C 29 DB : 07 3A 5B 73 : : B2 2C 97 4F : 51 0C 51 D3
768

Jeremy Fitzhardinge
jeremy@softway.com.au
C
C6 22 00 49 : B4 13 27 6A : : D1 EB 96 EF : 90 DF 29 1C
1024

Robert Frank
Berner Straße 1, D-81476 München, Germany
rfrank@golem.muc.de
http://www.vwl.uni-muenchen.de/~robert/
C
1F A3 41 2A : 90 57 A5 57 : : 90 FE A1 6F : 4A 77 91 31
1024

Martin Fredriksson
martin@msp.se
C
52 93 CF 6F : F8 82 74 4E : : 49 03 2A A2 : 5C FF 2F E8
1024

Matteo Frigo
MIT Laboratory for Computer Science
545 Technology Square, Cambridge, MA 02139, USA
athena@theory.lcs.mit.edu
http://theory.lcs.mit.edu/~athena
C
1995
5A 55 13 3A : AA BA 3D 57 : : 27 61 8A 01 : 94 8A 93 60

Kevin E. Fu
1115 Silverstone Rd.
Holland, MI 49424
fubob@mit.edu
http://www.mit.edu/~fubob/
B
2047
E1 83 68 C5 : 1D 46 17 17 : : 9C D5 E9 AB : D3 3B 1E B5

Eiji Furukawa
CAD Group, Fujitsu Limited
age@cad.fujitsu.co.jp
C
1024
44 CA F4 97 : 5F B6 E1 A3 : : 18 87 C2 47 : B4 EA 62 F3

Simson Garfinkel
simsong@pleasant.cambridge.ma.us
D
1024
68 06 7B 9A : 8C E6 58 3D : : 6E D8 0E 90 : 01 C5 DE 01

Douglas Gatchell
National Science Foundation - NSFNET (CISE/NCRI)
4201 Wilson Blvd., Room 1175, Arlington, VA 22230
Tel: +1 703 306 1950
Fax: +1 703 306 0621
dgatchell@lanl.gov
C
1024
CA EB C5 EC : D8 09 EA 2C : : FF B5 C1 AD : 2F E5 58 85

Matthias Geiser
Hoehtalstraße 13, CH-5408 Ennetbaden, Switzerland
geiser@dial.eunet.ch
C
1024
3C 59 DE 10 : DF D4 ED 57 : : E8 F4 19 A8 : B0 48 1F D2

Stephen P. Gibbons
Steve@AZTech.Net
C
2047
A6 BA 93 6F : 11 16 E3 3B : : 1F 0F C4 A8 : F3 2A 49 7C

Magnus Gislason
University of Iceland, Computing Services (RHI)
magnus@rhi.hi.is
http://www.hi.is/~magnus/
C
1024
3D 9F 50 DC : 84 56 AB FD : : F4 50 2F F5 : 26 1C BE C8

Steve Glanstein
mic@aloha.com
P. O. Box 22885, Honolulu, Hawaii 96823-2885, USA
AD C9 EC AA : D2 41 2D 60 : : 91 9A 66 0D : 56 B3 9E 03
C
1024

Constantin Gabriel Gonzalez
Muehlenstraße 120, D-38678 Clausthal-Zellerfeld, Germany
gonzalez@rz.tu-clausthal.de
http://home.tu-clausthal.de/~incg/
35 82 00 2E : 32 7A AB DE : : 5C 24 35 BC : 2D 97 22 B6
C
1024

Richard Gooch
Australia Telescope National Facility
PO Box 76, Epping NSW 2121, Australia
Tel: +61 2 9372 4387
rgooch@atnf.csiro.au
http://www.atnf.csiro.au/~rgooch/
34 29 30 4D : F4 79 C7 F7 : : 6A 45 B7 F7 : 74 59 39 9D
C
1024

David L. Good
dgood@rdatasys.com
38 F2 79 BF : 51 00 28 11 : : 73 A5 BA 85 : 54 8C 1F 60
C
768

Ian D. Goodyer
Wellcome Trust Centre for Human Genetics, University of Oxford
Windmill Road, Oxford OX3 7BN, United Kingdom
Tel: +44 1865 740020
Fax: +44 1865 742186
goodyer@pobox.com, goodyer@bigfoot.com
http://www.pobox.com/~goodyer
13 F8 C2 E6 : ED BB 21 93 : : 84 E3 0C A9 : 19 36 A8 BD
C
1024

Paul Gosse
paulg@charon.ucs.mun.ca
9C F9 86 50 : A3 26 19 97 : : 6D 97 C0 B5 : C3 F8 A8 F8
C
1024

Christian Graefe
christian@schokola.de
69 7B 85 B7 : 76 FC 96 BC : : CE AD D2 5A : 88 E0 53 40
C
1024

Christoph Graf
DANTE
Francis House, 112 Hills Road, Cambridge CB2 1PQ, United Kingdom
Tel: +44 1223 302992
Fax: +44 1223 303005
Christoph.Graf@dante.org.uk
http://www.dante.net
C3 04 FC F3 : 46 4E 27 D9 : : DE 09 61 F3 : 44 B9 4E E4 — **C** 1024

Lucky Green
shamrock@netcom.com
F0 B1 7B AE : 30 81 88 63 : : EA 00 1D 55 : 08 1F F9 38 — **C** 1024

Theo de Groot
T.deGroot@uvh.nl
7F D3 25 B3 : BD 9E BC DD : : 01 8D 54 27 : EE E9 95 22 — **C** 1024

Peter Gutmann
pgut1@cs.aukuni.ac.nz
7C 6D 81 DF : F2 62 0F 4A : : 67 0E 86 50 : 99 7E A6 B1 — **B** 1024

Per Hagen
Corporate Networking and Security
Aarhuus Stiftsbogtrykkerie
Søren Nymarks Vej 1, DK-8270 Hojbjerg, Denmark
hagen@well.com
A8 FD B3 C2 : 32 AC 01 4F : : D9 55 BF 05 : C3 1E 9B A3 — **C** 1024

Chris D. Halverson
Complete Internet Solutions
cdh@CompleteIS.com
http://www.completeis.com/~cdh/
3F 36 64 66 : 0C 53 A8 BC : : EE F0 AE AD : C7 3C 3F 19 — **C** 1024

Frederick S. Hann
1469 Bradshire Drive, Columbus, OH 43220, USA
fred@ratface.chem.pitt.edu
1C B3 AE DB : 5E CF 61 BB : : 82 9C 6E 9E : 17 D2 B9 B6 — **C** 1024

Ask Bjørn Hansen
Netcetera
Finsensvej 80 - DK-2000 Frederiksberg, Denmark
Tel: 38 88 32 22
Fax: 38 88 30 38
ask@netcetera.dk
http://www.plys.net/
DE E6 00 0E : B2 45 44 5C : : 1F FB 38 94 : 06 3A 0E B4 — **C** 1024

Svenn Agnar Hanssen
University of Tromsø
N-9037 Tromsø, Norway
Tel: +47 77 64 41 06
Fax: +47 77 64 41 00
svenn@hanssen.priv.no
http://www.cc.uit.no/~svenn/

C 1024

DE 9A D7 23 : 7C 82 14 F7 : : 9C 16 64 5B : 90 BD BA 4B

Steve Harris
steveha@compuserve.com

C 1024

D7 89 36 BA : 5F 5F 15 B7 : : 1A ED 22 93 : F7 0D 7A BE

Sam Hartman
hartmans@mit.edu

C 2047

E0 B9 B4 C1 : D8 29 7D 2F : : A3 85 B6 86 : 7E F1 71 36

Craig R. P. Heath
SCO
Croxley Business Park, Hatters Lane, Watford WD1 8YN, United Kingdom
craig@sco.com
http://ourworld.compuserve.com/homepages/strobie/

C 512

EF 54 3C 2B : F5 4D 7C 44 : : 01 64 19 FD : CE 47 E8 27

Roland Hedberg
Roland.Hedberg@umdac.umu.se

C 1024

A1 0E 8C 6F : 17 E4 EC 84 : : B0 8B D6 97 : 07 73 E3 A7

Jochen Hein
Frankenstraße 33, 34131 Kassel, Germany
Tel: +49 561 9324626
Jochen.Hein@delphi.central.de

C 1024

25 72 FB E3 : 85 9F DE 3B : : CB 0A DA DA : 40 77 05 6C

Arne Helme
Informatica/SPA, Univ. Twente
Box 217, 7500 AE Enschede, The Netherlands
Tel: +31 53 4894178
Fax: +31 53 4894590
arne@acm.org
http://www.huygens.org/~arne

C 1024

B8 34 6F 33 : E7 91 D7 D5 : : 46 30 00 6C : 9D FD 92 92

Boris Hemkemeier
Fachbereich Mathematik
Universitaet Dortmund, D-44221 Dortmund, Germany
Boris.Hemkemeier@Mathematik.Uni-Dortmund.DE
C
8C DE 6C 1D : 82 AF 04 13 : : 45 CF C4 6F : 5F 81 B6 93
1024

Heiner Heng
Hochschulrechenzentrum, Senckenberganlage 31-33
D-60054 Frankfurt/Main, Germany
Tel: +49 69 798 23917
Fax: +49 69 798 28817
heng@rz.uni-frankfurt.de
http://www.rz.uni-frankfurt.de/~heiner/
C
37 F8 41 FE : 63 00 1C DF : : 36 9E 40 4F : 7D 8C 25 8E
768

Frank Heyder
heyder@fmi.uni-passau.de
C
10 52 73 C6 : EA 66 3D 70 : : 0C C7 C4 A4 : 4A EF B0 1E
1024

Manfred Heyne
heyne@muenster.de
C
55 B6 BB 66 : 7F 2C DD 10 : : 65 2A 53 C4 : D1 3C A8 9E
1024

Jim Hickstein
jxh@jxh.com
C
2E F4 48 80 : 4E 6A 24 BF : : C9 2F CE 92 : EC 54 77 F9
1024

Roman Hodek
IMMD II
Roman.Hodek@informatik.uni-erlangen.de
http://www2.informatik.uni-erlangen.de/~rnhodek
C
6E 67 D0 5B : 8F 45 C1 14 : : 0B C3 22 CB : F4 B2 8B 54
1024

Peter Honeyman
Center for Information Technology Integration
University of Michigan, Ann Arbor, MI 48103, USA
Tel: +1 734 763 4413
honey@citi.umich.edu
http://www.citi.umich.edu/u/honey/
A
8C 96 31 78 : CD 85 26 2B : : B4 7D 5F 7A : B1 BD 9B 17
1024

Mike Horwath
drechsau@visi.com
C
D8 24 CC E6 : 47 5F E4 60 : : BF B7 6E FA : BF C7 6E C5
1024

Ari Hovila
Computer Centre, University of Vaasa
P.O.Box 700, 65101 Vaasa, Finland
ajh@UWasa.fi
http://www.uwasa.fi/~ajh/
C
8B 0E 8B A8 : BC B8 6F D6 : : B3 5E BB 6E : F5 A0 BE CF 768

Keith C. Howell
UUNET Technologies Inc.
3060 Williams Drive, Fairfax, VA 22031-4648, USA
kch@uu.net
C
67 25 99 E2 : 69 06 6E EA : : 5B 81 85 AE : 76 CB 68 3A 1024

Thomas E. Hutton
hutton@sand.net
http://www.sand.net/~hutton
C
FC 51 FE F0 : DB F2 EC BC : : 5D 54 7D F9 : 28 7E B2 A1 1024

Jens Immig
GECKO mbH Rostock (Germany)
GECKO mbH, Koch-Gotha-Str. 1, 18055 Rostock, Germany
Tel: +49 381 45488 31
Fax: +49 381 45488 50
jim@gecko.de
http://www.gecko.de
C
02 1C 06 EB : 2A 28 A3 EA : : 1E 09 EE 82 : 3F D0 A6 E4 1024

Ian Jackson
ijackson@chiark.greenend.org.uk
A
59 06 F6 87 : BD 03 AC AD : : 0D 8E 60 2E : FC F3 76 57 1024

Mark Jackson
AT&T Labs
mjackson@attmail.com
C
5B 99 AC C6 : DF 07 EC 55 : : 8C AB BF C7 : 53 B4 68 E0 1024

Kai-U. Jarius
Klinikstraße 58, 44791 Bochum, Germany
kai.u.jarius@ruhr-uni-bochum.de
C
BE 2B EB A4 : 08 AD A7 B4 : : EA 65 FE 34 : 11 35 4A 7C 1024

Tony Jarnstrom
tony@myself.com
http://www.iki.fi/t.j/
C
86 91 97 B5 : AF 16 5F 4B : : DB B1 78 10 : 94 28 3E E0 2047

Ruediger Jasse
Curslacker Heerweg 28, 21039 Hamburg, Germany
R_Jasse@poet.shnet.org
http://www.germany.net/teilnehmer/100/42956/index.html
0B C6 59 90 : DA E7 C5 F5 : : 8D 88 30 EB : 61 BB EF 57 — **C** 1024

Torsten Jerzembeck
Steinfurter Straße 79, Zi. 509, D-48149 Münster (Westfalen), Germany
Tel: +49 251 296039
Fax: +49 251 296039
toje@detebe.org
AB 6C B6 E8 : DE B8 15 F3 : : 2D 82 C2 B2 : E7 4A 55 98 — **C** 1024

Andy Johnston
ajohns5@alumni.umbc.edu
EE 5F 04 D7 : F0 A8 3F D8 : : 7B 33 BB 62 : 76 C0 6C 5E — **C** 1024

George M. Jones
CompuServe Internet Security
5000 Britton Rd., PO BOX 5000, Hilliard, Ohio 43026-5000 USA
Tel: +1 614 723 4560
Fax: +1 614 723 1221
George.Jones@CompuServe.NET
20 79 AE 12 : D0 8C 44 8F : : C5 37 2B 40 : EA F5 C3 35 — **C** 1024

LaMont Jones
Hewlett-Packard Company
lamont@hp.com
91 FD 12 DC : 32 17 F8 41 : : 02 5C 22 47 : FC BF 0E DE — **B** 1024

Börje Josefsson
Computer Centre
University of Luleå
S-971 87 Luleå, Sweden
Borje.Josefsson@dc.luth.se
http://www.dc.luth.se/~bj/
FB 64 50 FB : 7D 47 45 C5 : : 81 49 55 7A : 97 B8 4F C9 — **C** 2048

Tobias Kammann
tobias.kammann@informatik.uni-hamburg.de
3C 51 21 93 : 8F C8 46 31 : : 60 44 5D DE : 0D 02 99 F6 — **C** 1024

Karl-Johan Karlsson
Alsättersgatan 5C:25, 584 35 Linköping, Sweden
kj@lysator.liu.se
http://www.lysator.liu.se/~kj/
64 64 43 D5 : 1D FA B3 A5 : : 39 04 D4 7A : A4 37 1E A8 — **C** 1024

Phil Karn
karn@ka9q.ampr.org
http://people.qualcomm.com/karn
65 78 AF 09 : 6E 86 70 B5 : : 10 79 38 4B : 28 E6 92 06
B
1024

Jan "Yenya" Kasprzak
Fakulta informatiky MU, Botanicka 68a, 602 00 Brno, Czech Republic
kas@fi.muni.cz
0D 99 A7 FB : 20 66 05 D7 : : 8B 35 FC DE : 05 B1 8A 5E
B
1024

David M. Katinsky
dmk@sgi.com
43 C4 17 DF : 04 2B A7 4F : : 0E F7 12 62 : DA AE F1 F3
C
1024

Charlie Kaufman
Iris Associates
5 Techology Park Drive, Westford, MA 01886, USA
charlie_kaufman@iris.com
29 6F 4B E2 : 56 FF 36 2F : : AB 49 DF DF : B9 4C BE E1
C
1024

Andrew S. Kelley
kelleya@dim.com
BE B0 2A 49 : 68 01 F7 00 : : 0A B2 B9 67 : 3D 91 0E 60
C
1024

Stefan Kelm
DFN-PCA, University of Hamburg
Vogt-Kölln-Straße 30, 22527 Hamburg, Germany
Tel: +49 40 5494 2262
Fax: +49 40 5494 2241
kelm@pca.dfn.de
http://www.pca.dfn.de/~kelm/
81 75 AB 55 : C8 04 95 D0 : : 1A 6D FD 66 : 53 0B E6 6F
B
1024

Simon Kenyon
simon@itc.icl.ie
AC B0 8D 68 : 15 39 C0 AF : : 33 E7 25 82 : 4A 58 78 97
C
1024

Angelos D. Keromytis
Computer and Information Science department
University of Pennsylvania
Office 102E, Moore Building, 200 S. 33rd Street
Philadelphia, PA 10104-6389, USA
Tel: +1 215 573 3078
Fax: +1 215 573 2232
angelos@dsl.cis.upenn.edu
angelos@adk.gr
61 50 FD 51 : 8D FB F8 17 : : C8 A7 5A D1 : A2 45 C1 DD
A
1024

Thijs Kinkhorst
Molenstraat 28, 5327 AZ Hurwenen, The Netherlands
Tel: +31 418 664 055
thijs@kink.xs4all.nl
http://www.kinkhorst.com/ **C**
FD F7 2D 09 : 28 A0 80 01 : : B2 A5 A2 0E : 3F 2D 60 A2 1024

Olaf Kirch
Caldera
Darmstadt, Germany
okir@monad.swb.de **C**
56 4B 83 0C : AC D9 E5 54 : : FD 26 F5 80 : 56 9C 29 A2 1024

Tero Kivinen
kivinen@ssh.fi
http://www.iki.fi/kivinen/ **C**
F6 55 1D B3 : 12 D3 35 C4 : : AD 18 69 0D : F0 72 25 99 2048

Rolf Kleijnjan
technic@cybercomm.nl **C**
B9 88 19 39 : 34 63 6B AF : : 5D 2E A1 E8 : 9A 4F 70 81 2048

Daniel Kluge
Irringersteig 3, 8006 Zürich, Switzerland
dkluge@acm.org
http://www.vis.inf.ethz.ch/~daniel/ **C**
89 6E 2D 5E : CE 91 27 64 : : 3E E4 D3 96 : 7F 11 22 A7 1024

Sven Koch
haegar@ccc.de
http://www.ccc.de/ **C**
0F C6 E5 4B : FA 1E 08 29 : : 97 AA 62 D7 : 73 43 C4 73 1024

Werner Koch
werner.koch@guug.de **C**
62 9E 97 C0 : D5 55 76 3B : : 90 5A FA E9 : 81 1C 64 09 768

John Kohl
john_kohl@alum.mit.edu **C**
AC C3 22 F2 : E8 2F 87 8D : : A3 49 29 CA : CD 2E 71 89 1024

David Kok
davek@g7.org
http://g7.org/~davek **C**
79 24 B4 07 : FF 9E AC 17 : : CA 4C 74 67 : 46 71 4B 1D 1024

Petr Kokes
doktor@brn.pvtnet.cz
D8 D0 5F A8 : 77 F0 3A 44 : : 11 D9 A2 B4 : 89 93 82 03
C
1024

Nico de Koo
Computing Centre Delft University
dekoo@rc.tudelft.nl
8E C7 9F B2 : 78 43 24 74 : : AB B7 65 90 : 76 17 9D 02
C
1024

Wolfgang J. Kopp
Buchenstraße 28, D-85716 Unterschleißheim, Germany
kopp@naranek.camelot.de
http://home.pages.de/~kopp/
FC 32 0D 2B : C6 6D 35 C1 : : 10 29 E2 0C : 58 18 2A E3
C
2047

Heiner Kruener
hk@martian.ping.de
FC C2 9A 67 : 69 B1 E2 64 : : 0C 59 AB AA : 08 7E 0C 45
C
1024

Harald Krusekamp
Harald_Krusekamp@ms.maus.de
E7 4D 37 11 : 5F 64 69 0B : : 04 54 13 3A : 42 6B 19 E4
C
1024

Markus G. Kuhn
University of Cambridge, Computer Laboratory
Pembroke Street, Cambridge CB2 3QG, United Kingdom
Tel: +44 1223 334676
Fax: +44 1223 334678
Markus.Kuhn@cl.cam.ac.uk
http://www.cl.cam.ac.uk/~mgk25/
F0 49 0D 10 : F0 FA F6 5B : : E7 BC 78 54 : 5F 6E 46 2E
A
1024

Anand Kumria
wildfire@progsoc.uts.edu.au
http://www.progsoc.uts.edu.au/~wildfire/
27 2D C6 FA : 14 A4 08 B7 : : 19 C2 C9 B1 : BF EE 2B D4
C
1024

John Ladwig
jladwig@nts.umn.edu
93 67 C8 B8 : BA D7 7F 9D : : C0 6C 16 0F : 95 55 B2 C3
C
1024

Krista Lagus
krista@psych.helsinki.fi
http://www.iki.fi/krista/
79 C0 F6 F0 : 7E 66 9A AC : : 17 BE 5C 7B : 85 91 0D CF
C
1024

David Lamorski
dl@top.east.de
29 D9 84 C1 : 64 1F 8D 47 : : C1 B8 EF 97 : 4D 60 C6 1F
C 512

Hauke Lampe
Drosselweg 29, 21244 Buchholz, Germany
Tel: +49 4181 281338
Fax: +49 171 8931394
packbart@hs-net.shnet.org
http://www.geocities.com/Athens/3342/
7C D7 07 D9 : 23 9D 71 FC : : 7C F1 F7 E5 : 30 02 22 3D
C 1024

Jason Larke
jlarke@umich.edu
25 22 99 CA : A6 A6 17 0B : : 9D B7 AE C1 : 55 3D E8 9B
C 1024

Kristian Lass
kristian.lass@uni-essen.de
F8 C4 DE 62 : 0A 2B CD F6 : : EE D1 73 FF : 2D 5D 7F 7D
C 1024

Mark Laubach
PO Box 4065, Mountain View, California, 94040-0065, USA
laubach@ricochet.net
http://www.com21.com/bizcards/laubach.html
93 FB CE 3A : D8 3F 63 8D : : 3D 9B 5B 98 : 36 D4 F4 E1
C 1024

Erik Lawaetz
Ebone Inc.
P.O. Box 2505, Vermundsgade 5, 2100 Copenhagen, Denmark
Erik.Lawaetz@ebone.net
http://www.ebone.net/
90 36 B0 84 : 86 46 82 1C : : AB B0 5D A8 : 21 7F C2 7B
C 1024

A Owen V Le Blanc
Manchester Computing, University of Manchester
Manchester M13 9PL, United Kingdom
LeBlanc@mcc.ac.uk
http://www.man.ac.uk/~zlsiial
DC 60 81 A4 : 33 7F 95 40 : : D0 86 3B 51 : 48 0A AC 0E
C 1024

Andrew Lee
alee@slac.stanford.edu
3F 18 2E AF : 35 70 6D C5 : : 60 B9 AB D6 : AD 25 91 91
C 1024

Jong-Hyeon Lee
University of Cambridge, Computer Laboratory
Pembroke Street, Cambridge CB2 3QG, United Kingdom
Tel: +44 1223 334719
Fax: +44 1223 334678
Jong-Hyeon.Lee@cl.cam.ac.uk
http://www.cl.cam.ac.uk/~jhl21

A 1024
51 7B 32 A5 : 08 FA 8D B2 : : 3F 7B DA 8C : 73 17 95 15

Richard D. Lee
rdlee@sgi.com

C 1024
7B F0 B1 84 : F7 BC 3F F7 : : AA 90 85 6D : A9 7B 5E 0C

Thomas Lenggenhager
The Swiss Academic and Research Network - SWITCH-CERT
Limmatquai 138, CH-8001 Zurich, Switzerland
lenggenhager@switch.ch

C 1024
59 4D 14 95 : 9D 91 60 5F : : 60 5B 67 31 : A5 BD 6B 43

Christian Leutloff
Aachen, Germany
leutloff@debian.org
http://www.oche.de/~leutloff/

C 1024
62 ED A6 51 : FE 8D 2F 2E : : D5 A9 8C 79 : DC 74 DD 71

Keith B. Lewis
Monash University
Clayton 3168, VIC, Australia
keithl@mukluk.cc.monash.edu.au
http://www-personal.monash.edu.au/~keithl

C 1024
55 EC 7D CC : 08 00 AB 54 : : 78 00 D9 93 : D5 64 6B 08

Wolfgang Ley
DFN-CERT
Vogt-Kölln-Straße 30, 22527 Hamburg, Germany
Tel: +49 40 5494 2262
Fax: +49 40 5494 2241
ley@cert.dfn.de
http://www.cert.dfn.de/~ley/

A 1024
52 0C F9 96 : B1 5D BA 44 : : D9 B1 A9 26 : 44 8C 0D A0

Paul C. Leyland
Microsoft Research, Cambridge, United Kingdom
pcl@ox.ac.uk

New key **A** 1024
D0 B1 4C A7 : 74 80 12 14 : : D8 61 3C A1 : 16 A7 55 55

Old key **A**
CC 3C AD 64 : 40 30 AC E6 : : C1 C6 C5 FC : 83 F7 C2 D2 1024

Tony Li
tli@usc.edu **C**
EC 88 40 DE : E6 E7 35 70 : : 94 AD D8 86 : 35 B2 AA 80 2047

Britta Liedtke
Liedtke@cert.dfn.de **C**
B7 AF 01 25 : 75 2A 5D A9 : : F4 F5 8E 22 : FD 84 DE 47 1024

Tomas Liljebergh
Computerdepartment, University of Örebro
Fakultetsgatan 1, 701 82 Örebro, Sweden
Tel: +46 19 303167
Fax: +46 19 303475
tlh@hoe.se **C**
47 9E 88 A5 : 13 8E 04 1E : : 5F B6 31 CC : 59 7C 54 AC 1024

Mattias Lindblad
Lysator ACS
Björnkärrsgatan 7B:11, 584 36 Linköping, Sweden
matli@lysator.liu.se
http://www.lysator.liu.se/~matli **C**
71 23 D9 79 : 25 A3 50 C2 : : 5C 4B 01 7E : 83 28 9F DE 1024

Steen Linden
Ebone Inc.
P.O Box 2505, Vermundsgade 5, Dk-2100 Copenhagen, Denmark
Steen.Linden@ebone.net
http://adm.ebone.net/~sl/ **C**
17 E4 1E E9 : FA A0 16 BF : : C7 C8 30 9D : CE 7A 20 0E 1024

James J. Lippard
GlobalCenter, Inc.
1224 E. Washington St., Phoenix, AZ 85034, USA
Tel: +1 800 463 8386
Fax: +1 602 416 6111
lippard@skeptic.com **C**
35 65 66 9F : 71 FE 50 57 : : 35 09 0F F6 : 14 D0 C6 04 1024

Patrick J. LoPresti
MIT
patl@lcs.mit.edu **C**
21 94 72 0B : 61 04 58 F5 : : 49 D1 80 98 : B5 5C 5A CF 1024

Petr Machacek
Fakulta informatiky MU, Botanicka 68a, 602 00 Brno, Czech Republic
Tel: +420 5 41 512 346
xmachac@fi.muni.cz
92 27 25 77 : 08 A8 8D 3D : : AC B2 DD 9C : CA C1 04 C9 — **A** 1024

Ingo Macherius
TU Clausthal
Ingo.Macherius@TU-Clausthal.de
http://www.tu-clausthal.de/~inim/
6D F8 61 92 : A6 22 32 D5 : : 29 91 1D C7 : 47 BF 0F 28 — **C** 1024

Andrew Macpherson
Security Technology & Consulting
Nortel Plc, London Road, Harlow, Essex CM17 9NA, United Kingdom
Tel: +44 1279 402423
Andrew.Macpherson.1248566@nortel.co.uk
BA 5D 38 84 : 65 7D F6 A5 : : 95 A7 20 1B : 81 2A 6E 42 — **C** 768

Nils Magnus
University of Kaiserslautern, Germany
Tel: +49 631 205 2166
magnus@unix-ag.uni-kl.de
http://wwwagr.informatik.uni-kl.de/~magnus/
B5 6D 0F 11 : D1 CE 59 2A : : CB 50 9C B7 : 27 96 80 DD — **C** 1024

Johan Magnusson
Björnkärrsgatan 7 C:12, 584 36 Linköping, Sweden
johan@lysator.liu.se
http://www.lysator.liu.se/~johan
1F 3D 82 0E : BB D5 09 8F : : 38 2D 78 D9 : BF 73 50 7E — **C** 1024

Andrew Main
zefram@fysh.org
39 56 CF C8 : CC 00 11 92 : : E5 01 93 1B : D9 48 38 B5 — **C** 2048

Niko Mäkilä
nmakila@research.nokia.com
19 C1 B2 C3 : 28 FE 35 EB : : B6 C5 55 34 : 35 15 8C F3 — **C** 1024

Chris Maltby
Softway Pty. Limited
PO Box 305, Strawberry Hills NSW 2012, Australia
Tel: +61 2 9698 2322
Fax: +61 2 9699 9174
chris@sw.oz.au
http://www.softway.com.au/~chris

C
1024

B0 4D AD F5 : B8 2A 43 26 : : 58 41 74 BF : 36 5F 41 20

Peter Mandrella
Sudetenstraße 10, D-69221 Dossenheim, Germany
pm@daisy.de
http://www.daisy.de/pm

C
512

A4 4E 07 AB : 41 58 4E C7 : : BF 0F 8A D7 : BF 74 3D 6F

Charalampos Manifavas
University of Cambridge, Computer Laboratory
Pembroke Street, Cambridge CB2 3QG, United Kingdom
Tel: +44 1223 334676
Fax: +44 1223 334678
Charalampos.Manifavas@cl.cam.ac.uk
http://www.cl.cam.ac.uk/~cm213

A
1024

D4 BF D5 6C : 86 83 EC 37 : : 88 B1 8E 92 : 9D 9A 97 FA

John Mann
Network Services Activity, Computer Centre, Monash University
Clayton, Victoria 3168, Australia
Tel: +61 3 990 54774
Fax: +61 3 990 54746
John.Mann@cc.monash.edu.au
http://www-personal.monash.edu.au/~johnm/

C
1024

16 94 33 9F : 85 C2 5A E4 : : 6E DB 0F 26 : 9B 8A AD 81

Dale E. Martin
University of Cincinnati
dmartin@ececs.uc.edu
http://www.ececs.uc.edu/~dmartin

C
1024

BB AC 36 BF : 95 EE AC 85 : : FD 29 0C 08 : E1 97 B9 5A

Eric Maryniak
Lange Hofstraat 3, 2011 DK Haarlem, The Netherlands
eric.maryniak@niwi.knaw.nl
http://huizen.dds.nl/~maryniak/

C
1024

BA 86 32 EC : 9B 25 F3 62 : : 20 45 1C A6 : AB 2B 8D E6

Leslie Todd Masco
HKS.net
6332 Forward Ave, #1 Pittsburgh PA 15217, USA
cactus@hks.net
http://www.hks.net/~cactus/
C
1024
9D 08 B1 F6 : F4 4C F3 9C : : 45 A0 CD DB : 58 08 41 A9

Lars Henrik Mathiesen
Danish Computing Centre for Research and Education (UNI-C)
Vermundsgade 5, DK - 2100 Kobenhavn, Denmark
Tel: +45 35 87 88 68
Fax: +45 35 87 88 90
Lars.Henrik.Mathiesen@uni-c.dk
C
1024
51 89 68 F6 : 1B 80 60 80 : : DA 54 7D 3C : 5B 66 75 DA

Václav Matyáš Jr.
University of Cambridge, Computer Laboratory
Pembroke Street, Cambridge CB2 3QG, United Kingdom
Tel: +44 1223 334719
Fax: +44 1223 334678
Vaclav.Matyas@cl.cam.ac.uk
http://www.cl.cam.ac.uk/~vm206
A
1024
C3 CB 4E FD : 9E DE F0 CA : : 65 D5 BF 7C : 46 8F 7B 5C

Lionel J Mauritson Jr
lionel@mauritson.com
http://www.mauritson.com/lionel/
C
1264
66 2A 82 9B : 4B B2 85 9B : : F8 D8 5E EF : F6 39 C8 7D

Simon D. McAuliffe
PO Box 3453, Wellington, New Zealand
Tel: +64 4 384 4860
S.McAuliffe@dtsp.co.nz
C
1024
65 5B B4 6C : CB 6A 65 F1 : : 01 91 B9 FE : 34 23 99 D3

Aubrey McIntosh
Chemistry Dept., University of Texas at Austin
A5300, Austin TX 78712, USA
mcintosh@ccwf.cc.utexas.edu
http://ccwf.cc.utexas.edu/~mcintosh
B
1024
C6 D9 AE 3A : 39 3B B0 D6 : : B5 4B 07 03 : 40 AB 48 D0

Kevin J. McMahon
MCI Technical Security
Kevin.J.McMahon@mci.com
C
1024
85 5F 8A 73 : 7C 42 D4 C5 : : AB B5 3B C7 : D9 EF ED 55

Erich Meier
IMMD IV, University of Erlangen
Martensstraße 1, 91058 Erlangen, Germany
Tel: +49 9131 85 8026
meier@informatik.uni-erlangen.de
http://www4.informatik.uni-erlangen.de/~meier/
C 1024
64 88 E8 0A : 02 EA 6A D6 : : 42 A9 13 5B : 7B E3 1D 08

Alexander Meisel
meisel@ai-lab.fh-furtwangen.de
http://www.ai-lab.fh-furtwangen.de/~meisel/
C 1024
9C C4 DE AE : 9A 1D CC 18 : : 40 60 48 4C : BA FD 60 D9

Scott Merrilees
BHP Information Technology
PO Box 216, Hamilton, NSW 2303, Australia
Sm@itntl.bhp.com.au
C 1024
67 DC F8 08 : 48 27 77 7D : : C0 4B 44 35 : 9F 18 9A 7F

Stefan Merten
merten@dfki.uni-kl.de
C 1024
82 58 69 3A : 96 A8 F7 9E : : 0E 3E 2F 23 : 70 A4 8F DB

Charles H. Mingo
54 Barrow Street #5C, New York, NY 10014-3768, USA
mingo@panix.com
http://www.panix.com/~mingo
C 1024
40 33 46 21 : E5 8F AA 52 : : 1E 0D 6D F3 : BB 86 AC 58

Ari Moisio
Niittykatu 7, 41160 Tikkakoski, Finland
armoi@sci.fi
http://www.arlainst.fi/~arimo
C 1024
8A 91 96 E2 : 98 64 D0 4D : : 57 5E 3E EE : 72 E9 DD D2

Oliver Moldenhauer
Alt Nowawes 64, 14482 Potsdam, Germany
o.moldenhauer@jpberlin.de
http://www.pik-potsdam.de/~oliver/
C 1024
EA B3 D8 37 : 23 CE 33 08 : : 77 CC 22 4B : 37 45 02 7D

Daniel Möllenbeck
Beethovenstraße 115
46145 Oberhausen, Germany
Tel: +49 208 610989
Fax: +49 208 610991
d.moellenbeck@gmx.de
00 9A DE BA : 38 3A 96 A0 : : 36 9F 0F DB : 77 62 C6 01 — **C** 1024

Bodo Möller
3moeller@informatik.uni-hamburg.de
C7 AC 7E AD : 56 6A 65 EC : : F6 16 66 83 : 7E 86 68 28 — **C** 1024

Ulf Möller
Hamburg, Germany
ulf@fitug.de
http://www.fitug.de/ulf/
B6 4F 97 28 : 8F C0 54 C3 : : A6 10 02 2F : B9 31 78 14 — **C** 1024

Stefan A. Mühlenweg
DFN-CERT
Vogt-Kölln-Str. 30, D-22527 Hamburg, Germany
Tel: +49 40 5494 2262
Fax: +49 40 5494 2242
Muehlenweg@cert.dfn.de
http://www.cert.dfn.de/team/sam/
D9 B8 16 23 : 26 D7 26 15 : : E8 AC 42 DE : F2 34 B0 7B — **B** 1024

Dirk Müller
Schillerstr. 57, 48155 Muenster, Germany
Tel: +49 251 664639
dirk@ldp.westfalen.de
62 A9 6E CD : AC 2E 0F A4 : : EE 83 29 61 : AD AD FD C9 — **C** 1024

Rene Müller
rene@math.fu-berlin.de
http://www.math.fu-berlin.de/~rene
22 71 97 61 : 92 AC BF E5 : : 8A 99 01 89 : BF 4F 69 8C — **C** 1024

Uwe Münch
muench@ph-cip.uni-koeln.de
http://www.ph-cip.uni-koeln.de/~muench/
79 5B C8 D8 : 03 E2 11 98 : : 56 EC 53 36 : 59 58 3D 9B — **C** 1024

Simo Muinonen
smm@iki.fi
http://www.iki.fi/smm/
6F 7C 72 6C : E3 31 12 AF : : FC 9E 49 C6 : 32 A6 FC FF — **C** 1020

Christopher T. Nadovich
1302 Diamond Street, Sellersville, PA 18960 USA
Tel: +1 215 257 8708
Fax: +1 215 257 8154
chris@jtan.com
http://www.jtan.com/chris/

C 512

7D F1 0B EC : B6 AB EC 88 : : 0A D8 AA BF : 74 A0 2C 0A

Jens Nedon
1nedon@informatik.uni-hamburg.de

C 1024

C7 16 D6 9F : C9 C8 F1 31 : : 71 02 12 B7 : 03 58 BC 69

B. Clifford Neuman
Information Sciences Institute, University of Southern California
4676 Admiralty Way, Marina del Rey, California 90292-6601, USA
bcn@isi.edu
http://www.isi.edu/people/bcn

C 1024

09 26 EB 64 : 47 2C 6B 34 : : 48 34 03 AA : 63 4B AE 71

Teun Nijssen
Tilburg University
Teun.Nijssen@kub.nl

C 1024

61 C5 B0 E5 : D9 0B 5A 33 : : 09 E4 52 EC : CD EA 6F 2D

Landon Curt Noll
Silicon Graphics Inc.
chongo@sgi.com

C 1024

D4 30 55 08 : 41 76 BA 15 : : 03 87 29 9B : B6 17 91 4C

Brent J. Nordquist
5637 - 10th Ave. S., Minneapolis, MN 55417-2403, USA
bjn@visi.com
http://www.visi.com/~nordquis

C 1024

15 80 4B 05 : 14 33 69 AD : : 02 BB 78 B5 : 75 8F 07 73

Andy Norman
Hewlett-Packard Laboratories
ange@hplb.hpl.hp.com
http://www-uk.hpl.hp.com/people/ange

C 1024

DE 80 0B 25 : E3 7B D9 60 : : EA F3 65 A2 : E2 EC 93 F6

Göran Öberg
Luleå University of Technology, Sweden
Goran.Oberg@dc.luth.se
http://www.luth.se/~goggi/

B 2048

26 D3 F1 42 : AE 99 3B F6 : : C3 E5 9D 58 : E9 1E C3 2E

David E. O'Brien
The NUXI BSD Group
obrien@FreeBSD.org
B7 4D 3E E9 : 11 39 5F A3 : : 90 76 5D 69 : 58 D9 98 7A
C
1024

Tim O'Connor
111 Barrow Street, #4E, New York, NY 10014, USA
tim@roughdraft.org
http://www.roughdraft.org/
B7 58 49 3D : 25 30 F5 68 : : F8 51 85 6A : 2B A4 E5 4F
B
1248

Bill O'Donnell
billo@billo.com
DE B8 46 22 : 3C DD 07 E7 : : 82 42 CF 43 : 0B A7 E2 59
C
1024

Marius Olafsson
University of Iceland
Taeknigardi, Dunhaga 5, 107 Reykjavik, Iceland
Tel: +354 525 4747
marius@hi.is
0B 4C D2 08 : 4E A0 66 AE : : 8B 1A 1E DF : 76 29 43 62
C
512

Richard W. Outerbridge
50 Walmer Road #111, Toronto, Ontario, Canada M5R 2X4
Tel: +1 416 961 4757
Fax: +1 416 961 9617
outer@interlog.com
6A 89 D4 9F : D3 DA 12 E4 : : 04 0A 27 3B : F3 83 01 27
A
1024

Keith Owens
Keith_Owens@ocs.com.au
http://www.ocs.com.au/~keith
2B 25 0A 31 : 02 AE CA F7 : : 73 0C 28 69 : 4A 7B 65 27
C
917

James E. Pace
jepace@pobox.com
http://www.pobox.com/~jepace
8C E7 12 5A : 3A 8C 5C 4D : : EC 15 7B 65 : EA 82 D2 BF
C
1024

Marcel van der Peijl
bigmac@xs4all.nl
F8 94 E4 4C : 2A 6A B1 6C : : F1 41 4E 22 : D7 4F 96 BD
C
1024

Xavier Perramon
Universitat Politècnica de Catalunya, Dept. Arquitectura de Computadors
Campus Nord, Edif. D6, C. Jordi Girona 1-3
E-08034 Barcelona, Spain
perramon@ac.upc.es
http://sirius.ac.upc.es/~xavi/
C 768
43 A3 06 89 : E3 14 CC 85 : : 75 D9 7F E4 : 39 5A 81 D5

Fabien A.P. Petitcolas
University of Cambridge, Computer Laboratory
Pembroke Street, Cambridge CB2 3QG, United Kingdom
Tel: +44 1223 334676
Fax: +44 1223 334678
Fabien.Petitcolas@cl.cam.ac.uk
http://www.cl.cam.ac.uk/~fapp2
A 1024
27 09 EB 53 : 98 99 B2 8B : : CA DB AC 31 : CC FD 2B 1B

Birgit Pfitzmann
Universität des Saarlandes
Fachbereich Informatik, Im Stadtwald, Geb. 45, R. 536
D-66123 Saarbrücken, Germany
Tel: +49 681 3025631/0
Fax: +49 681 3024631
pfitzmann@cs.uni-sb.de
http://www.semper.org/sirene/people/birgit/info.birgit.html
A 1024
AA 52 36 26 : 37 4F 34 2F : : 5F 25 9E A6 : 57 D9 9A 80

Florian Piekert
Rheinring 68, 38120 Braunschweig, Germany
Tel: +49 531 864781
Fax: +49 531 863917
floppy@floppy.org
http://www.floppy.org
C 1024
72 E9 D4 2A : 51 E8 29 CA : : EE 42 60 29 : 5E F6 E9 AB

Melvin J. Pleasant Jr.
Silicon Graphics Inc.
pleasant@sgi.com
C 1024
61 F9 CB D8 : 2E 13 17 F1 : : 8A 97 93 E6 : 29 50 16 F4

Paul Pomes
QUALCOMM, Inc
6455 Lusk Blvd
San Diego, CA 92121, USA
ppomes@qualcomm.com
http://people.qualcomm.com/ppomes/
C
1024
0E 12 63 81 : 06 81 45 BC : : BD C1 1B F5 : 27 A0 C6 7B

Johannes Posel
posel@gmx.net
http://homepages.munich.netsurf.de/Peter.Posel/
C
1024
4B D1 F1 39 : B4 B7 B3 EB : : 1B 3E E8 53 : 9A 9C 76 8B

Geraint Price
University of Cambridge, Computer Laboratory,
Pembroke Street, Cambridge CB2 3QG, United Kingdom
geraint.price@cl.cam.ac.uk
http://www.cl.cam.ac.uk/~gp200
A
1024
12 4A 01 86 : 72 16 B7 48 : : F5 E4 6C CA : 2C 57 6C CA

Mark Prior
connect.com.au pty ltd
Level 1, 45 Pirie Street, Adelaide, SA 5000 Australia
Tel: +61 8 8203 2088
Fax: +61 8 8203 2099
mrp@connect.com.au
http://www.connect.com.au
C
1024
7D FE 0C 28 : 4D F7 66 76 : : AA 1D 1E 19 : D0 D1 33 AC

Niels Provos
PHYSnet Rechnerverbund, Universität Hamburg
Jungiusstraße 9, 20355 Hamburg, Germany
Tel: +49 40 4123 2404
Fax: +49 40 4123 6571
provos@physnet.uni-hamburg.de
http://www.physnet.uni-hamburg.de/provos/
B
1024
A6 88 52 81 : A5 A8 89 49 : : 2D 8A 60 34 : 42 D8 87 DE

Damir Rajnovic
Damir.Rajnovic@ukerna.ac.uk
C
1024
B8 DB C6 85 : FE B2 93 89 : : 17 46 09 2A : CD 65 55 A1

Hans Ranke
Ranke@Regent.E-Technik.TU-Muenchen.DE
C
1024
62 5D B2 0B : EF BF 7B E4 : : 30 F6 B9 32 : 1A 66 6D 56

Felix Rauch
Institute for Computer Systems /RZ H15
ETH Zentrum, 8092 Zürich, Switzerland
rauch@inf.ethz.ch
http://www.cs.inf.ethz.ch/~rauch/
C
F4 71 A9 C4 : A4 4D B5 9A : : F0 77 B6 DA : F4 A9 63 FE
1024

Jack Repenning
Informix Software Inc., Config/Release Mgmt
4100 Bohannon Drive, M/S: 4100/2, Menlo Park, CA 94025,USA
Tel: +1 650 926 1044
Fax: +1 650 926 6571
jackr@informix.com
http://u2.netgate.net/~jack/
C
D2 4B E2 C2 : 9A FB 7C 24 : : 7E 59 78 85 : 52 5D 64 4E
1024

Joe Rhett
Navigist
jrhett@navigist.com
http://www.navigist.com/Staff/JRhett/
C
C7 9B BC 6C : 75 3D 96 8A : : 88 9C 11 35 : 89 CD DC CC
1024

Matthew Richardson
I.T.Consultancy Limited
Jersey, Channel Islands, British Isles
matthew@itconsult.co.uk
http://www.itconsult.co.uk
C
BC DB 9E 23 : 7B 76 4E 8E : : F4 05 BC 6F : 8A D7 1B 0D
1024

Timo J. Rinne
SSH Communications Security Ltd
Tekniikantie 12, FIN-02150 Espoo, Finland
tri@iki.fi
http://www.iki.fi/tri/
C
7E B6 1F E3 : 97 1D C8 F2 : : BC 9B 2C 46 : 76 73 60 5C
1024

Stefan Röhrich
Kornblumenweg 11, D-78465 Konstanz, Germany
sr@linux.de
http://home.pages.de/~sr/
C
49 1F 7A 5C : 59 5F 91 BD : : E1 76 4C FE : 1B 7E BC A1
2048

Thomas Roessler
Nordstraße 99, 53111 Bonn, Germany
roessler@guug.de
http://home.pages.de/~roessler/
C
AE 24 38 88 : 1B 45 E4 C6 : : 03 F5 15 6E : 9C CA FD DB
1280

Christian von Roques
roques@pond.sub.org
18 42 C0 CE : DB 2A 7E E0 : : A9 ED D9 64 : 8A 5C A2 0F
C 1024

Joel Rosdahl
Björnkärrsgatan 13 C:41, 584 36 Linköping, Sweden
joel@debian.org
http://rosdahl.ml.org/joel/
C5 65 0B F2 : 27 12 4C DC : : 1D 2B E7 65 : DD 35 E2 C8
C 768

Gregory G. Rose
QUALCOMM Australia
6 Kingston Avenue, Mortlake NSW 2137, Australia
Tel: +61 2 9743 4646
Fax: +61 2 9736 3262
ggr@qualcomm.com
http://people.qualcomm.com/ggr/
B5 DF 66 95 : 89 68 1F C8 : : EF 29 FA 27 : F2 2A 94 8F
B 1024

Roland Rosenfeld
Alemannenweg 15, 53332 Bornheim, Germany
roland@spinnaker.rhein.de
http://www.rhein.de/~roland/
2D E7 CC DE : D5 8D 78 BE : : 3C A0 A4 F1 : 4B 09 CE AF
C 1024

Jan G. Saell
YASK Systemkonsult AB
Box 59, S-692 21 Kumla, Sweden
Tel: +46 19 58 25 15
Fax: +46 19 58 38 05
jan@yask.com
BF 50 83 99 : C5 33 90 F2 : : 3D AA 0C FA : A9 A5 92 3B
C 512

Shabbir J. Safdar
shabbir@panix.com
69 38 12 3E : 6F 27 33 08 : : FC B5 34 63 : 47 D7 1D 4E
C 1024

Roger A. Safian
r-safian@nwu.edu
12 0C 13 0B : A3 A5 54 36 : : 45 93 08 00 : D4 E9 AA 0E
C 1024

Ilkka Salminen
Tel: +35 8405267660
ike@iki.fi
http://www.iki.fi/ike/
52 52 C8 5D : FC 7B B9 6B : : EC 45 D0 3F : 54 FC A3 17
C 1024

Ulla Sandberg
ulla@stupi.se
21 18 0C C5 : 83 80 28 96 : : 5F 28 0C 26 : 79 CE 48 A5 — **C** 1024

Kevin Sartorelli
kevin@sartorelli.gen.nz
AC 92 9C D3 : F1 F8 7E F2 : : 77 BF 97 8C : 16 F3 8A 97 — **C** 1024

Jeffrey I. Schiller
jis@mit.edu
http://bs.mit.edu:8001/~jis/home.html

_
BF 26 FA 39 : 50 04 5C BF : : 80 51 E3 52 : 4A 16 DF 96 — **B** 512

_
DD DC 88 AA : 92 DC DD D5 : : BA 0A 6B 59 : C1 65 AD 01 — **B** 1024

Jakob Schlyter
Computer Communications Group
Chalmers University of Technology, SE-412 96 Goteborg, Sweden
Tel: +46 31 772 59 19
Fax: +46 31 772 59 22
jakob@cdg.chalmers.se
http://www.cdg.chalmers.se/~jakob/
8E C1 A4 90 : 70 E3 FF EC : : E8 98 DB 39 : 43 18 D0 9D — **C** 1024

David M. Shaw
3501 St. Paul Street, #727, Baltimore, MD 21218, USA
dshaw@jabberwocky.com
http://www.jabberwocky.com/
7E 5D 6F 6D : 48 85 0B B7 : : B4 02 85 4E : 43 E8 8D 36 — **C** 2048

Mark E. Shoulson
shoulson@cs.columbia.edu
EF AE 80 E1 : D7 3E F6 8F : : 71 AE 0F 26 : 81 4F 90 84 — **C** 1024

Veikko Siivola
University of Helsinki
vsiivola@cc.helsinki.fi
http://www.helsinki.fi/~vsiivola/
04 A3 CF 60 : 03 FA 41 EE : : 34 48 BE AA : E1 6E 42 5E — **C** 1024

Dave Sill
Oak Ridge National Laboratory
PO Box 2008 MS6394, Oak Ridge, TN 37831-6394, USA
de5@ornl.gov
http://web.infoave.net/~dsill

C 2048
`44 34 D9 6D : C7 EB 83 C0 : : 19 7E A4 62 : 38 C2 5B 9F`

Nick Simicich
32 SW 12th Way, Boca Raton, FL 33486, USA
njs@scifi.squawk.com

C 1024
`21 8D AB A9 : 88 B6 3E 4B : : 34 4A 93 87 : BC C2 4E 53`

Geoff Simmons
MCS Moorbek Computer Systeme GmbH
Essener Straße 99, D-22419 Hamburg, Germany
gs@cityline.net
http://www.cityline.net/~geoff/

C 1024
`58 0B F5 90 : CC 82 DD 1D : : 94 54 C2 D9 : 0B C5 C6 CB`

Peter Simons
Ankerstraße 13, 53757 St. Augustin, Germany
Tel: +49 2241 921420
Fax: +49 2241 921429
peter.simons@acm.org
http://home.pages.de/~simons/

C 1024
`38 1D 9C DC : C8 B8 B3 ED : : CC 30 54 AD : EC A6 12 61`

William Allen Simpson
1384 Fontaine, Madison Heights, Michigan USA 48071-4818
wsimpson@greendragon.com

C 1024
`17 40 5E 67 : 15 6F 31 26 : : DD 0D B9 9B : 6A 15 2C 32`

Alexander W. Skwar
Digital Projects
Staasstr. 11, 42369 Wuppertal, Germany
Tel: +49 2022461967
ASkwar@DigitalProjects.com
http://www.digitalprojects.com

C 2047
`DA 45 2B B9 : DD 77 45 DD : : E8 3B BE 7E : 32 B9 EE C1`

Douglas Song
University of Michigan
P.O. Box 4296, Ann Arbor, MI 48106, USA
dugsong@umich.edu
http://www-personal.umich.edu/~dugsong/

B 2048
`BF F5 20 EA : DA 2F C4 F4 : : 7D 68 4A 50 : E4 35 D1 17`

Eugene H. Spafford
spaf@cs.purdue.edu
http://www.cs.purdue.edu/people/spaf
B
1024
9F 30 B7 C5 : 8B 52 35 8A : : 42 4B 73 EE : 55 EE C5 41

Tage Stabell-Kulø
Department of Computer Science, IMR
9037 Universitetet i Tromsø, Norway
Tel: +47 776 44032
Fax: +47 776 44580
tage@acm.org
http://www.cs.uit.no/~tage/
C
1024
C5 85 7D 10 : FC F2 3C 0F : : 73 E1 C0 00 : 83 CB 03 55

Francesco Stajano
Olivetti & Oracle Research Laboratory
24a Trumpington Street, Cambridge CB2 1QA, United Kingdom
Tel: +44 1223 343000
Fax: +44 1223 313542
fstajano@orl.co.uk
http://www.orl.co.uk/~fms
A
1024
E1 18 38 AF : FA F6 37 AC : : 48 74 9D 1F : 3F C3 2F B0

Bernard Steiner
UUNET Deutschland GmbH
Emil-Figge-Straße 80, D-44227 Dortmund, Germany
Bernard.Steiner@de.uu.net
C
1024
57 50 3A C1 : 95 71 5B 37 : : 3A 7D B3 D0 : 5F 1F 60 36

Michael Steiner
IBM Research Division, Zurich Research Laboratory
Saeumerstrasse 4, CH-8803 Rueschlikon, Switzerland
Tel: +41 1 724 8286
Fax: +41 1 724 8955
steiner@acm.org
http://www.zurich.ibm.com/~sti/
C
1024
D4 25 4E 05 : D3 3F 3E 2A : : 7B A0 94 39 : 73 40 C2 35

Don Stikvoort
PO Box 19035, NL 3501 DA Utrecht, Netherlands
don@surfnet.nl
http://surver.wind.surfnet.nl/~donus/
C
1024
05 EE A8 89 : 3B C1 17 7A : : 6B 2A BA 4F : 8B EB B4 A4

Suzana Stojakovic-Celustka
CARNet Infrastruktura
NSK, Hrvatske bratske zajednice bb, 10000 Zagreb, Croatia
Tel: +385 1 6164 355
Fax: +385 1 6164 395
Suzana.Stojakovic-Celustka@CARNet.hr
A7 9B C1 26 : 57 FE B0 BA : : CD 5F 0F C6 : 54 96 31 3E — C 1024

Ksawery Stojda
Gorczewska 88a m 11, 01-117 Warszawa, Poland
Tel: +48 602 222893
KStojda@Fore.com
CA 51 D4 CE : F3 A2 C2 24 : : 13 0E 66 45 : FE CA 71 04 — C 1024

John P. Studarus
9481 Questa Pointe, San Diego, CA 92126, USA
studarus@praja.com
96 22 CA B8 : E1 BB B4 AD : : CA 30 63 D8 : 5C 4A CB F6 — C 1024

Kimmo Suominen
Trans-Atlantic Communications
235 West 19th Street #1B, New York, NY 10011-4080, USA
kim@tac.nyc.ny.us
http://www.tac.nyc.ny.us/~kim/
6D 67 7B 0A : 3D B0 B7 60 : : 67 78 7C C0 : 03 40 A8 46 — C 1024

Edgar W. Swank
San Jose, CA 95123, USA
EdgarSwank@Juno.com
http://members.tripod.com/~EdgarS/index.html
54 80 BD 2A : C7 82 5E DB : : 1C 65 7A C2 : 14 C7 49 A3 — C 1024

Douglas M. Swiggum
Swiggum@Waisman.Wisc.Edu
50 DA 1E 68 : 2E 49 DC F3 : : FC E9 CD B1 : 78 CE 85 C2 — C 1024

Greg A. Tapolow
gt42+@pitt.edu
4D 8F 31 A1 : E6 69 CD D3 : : 77 F6 B4 74 : 10 40 C8 2A — C 1024

Eric Thompson
eja@cix.co.uk
CB FC 6B 29 : AA BB 00 32 : : C3 E1 58 7F : FF 83 2C FF — C 1024

Karsten Thygesen
Rebildparken 154, DK-9220 Aalborg, Denmark
karthy@SunSITE.auc.dk
http://sunsite.auc.dk/~karthy
C
12 A6 8F F1 : 86 91 E8 2A : : 48 B3 03 7D : 84 16 0F 11 1024

Win Treese
Open Market, Inc.
245 First St., Cambridge, MA 02142 USA
treese@OpenMarket.com
C
B3 A6 C1 54 : 57 38 74 C1 : : 2A 9B 22 A3 : 23 9B E8 D0 768

Gregory D. Troxel
gdt@lexort.com
C
C5 B4 47 A2 : 8B 4F 40 3D : : D8 25 2C F6 : 26 C7 DE CF 1024

Mark Turner
Kram
Burwell, Cambridge, England
markt@pipex.net
C
C2 BC F9 5E : 27 B5 1C 47 : : 00 FD F2 6B : D7 0B BE A4 1024

Stephen C. Tweedie
sct@dcs.ed.ac.uk
C
E2 FE A4 20 : 34 EC ED FC : : 7D 7E 67 8D : E0 31 D1 69 1024

Tapio Väättänen
Tel: +358 50 566 0220
tav@iki.fi
http://www.iki.fi/~tav/
C
54 B5 04 42 : 19 52 74 93 : : 04 AF CB 10 : C5 A2 53 5C 768

Jonathan J. Vafai
Dept. of Chemistry, New York University
31 Washington Place, New York, NY 10003, USA
vafaij01@mcrcr.med.nyu.edu
http://www.nyu.edu/~jjv200/
C
C8 4C DE CA : 8E 79 B3 87 : : 92 B6 A4 B0 : 72 CA C4 6E 768

Aldo Valente
valente@cs.bonn.edu
C
10 49 AF 70 : D5 49 3F AA : : 3B BF B1 FF : 82 13 6F 40 1024

Christopher Vance
Christopher.Vance@adfa.oz.au
C
4B 1E F2 79 : E8 2D 14 BC : : 67 0A D6 1F : AF 9C 3B 13 1024

Wietse Venema
wietse@wzv.win.tue.nl
B
1022
78 96 4A 4D : F0 F0 D1 3C : : 45 E9 03 FC : 17 67 DC D8

Ton Verschuren
SURFnet bv
Radboudburcht, P.O. Box 19035, 3501 DA Utrecht, NL
Tel: +31 302 305 305
Fax: +31 302 305 329
Ton.Verschuren@SURFnet.nl
C
1024
DE E3 2A BF : 65 63 48 5A : : 20 59 8F 16 : 6D C1 4B 94

Paul Vixie
HC 1 Box 159A, Woodside, CA 94062, USA
paul@vix.com
C
1024
BA A8 64 76 : 55 C1 72 63 : : 44 56 B2 0C : 07 E6 28 81

Alf Wachsmann
DESY-IfH
Platanenallee 6, D-15738 Zeuthen, Germany
Tel: +49 33762 77 363
Fax: +49 33762 77 216
alf@ifh.de
http://www.ifh.de/~alf
C
1024
46 ED B1 1E : 3B 1C 26 32 : : 44 1A 09 40 : 9E E4 B4 2D

Stefan Wagner
Tel: +49 172 691 9883
Stefan.Wagner@frankfurt.netsurf.de
http://people.frankfurt.netsurf.de/Stefan.Wagner
C
2048
57 D4 2D 57 : 05 0A DE 12 : : 9E FC B0 BC : 3A 0D E3 41

Michael Waidner
IBM Research Division, Zurich Research Laboratory
Saeumerstrasse 4, CH-8803 Rueschlikon, Switzerland
Tel: +41-1-724 8220
Fax: +41-1-724 8955
wmi@zurich.ibm.com
http://www.zurich.ibm.com/~wmi/
B
1024
1B 6D A7 26 : 09 69 D2 3D : : 79 86 9C F6 : 13 92 F4 29

Marcel Waldvogel
Computer Engineering and Network Laboratory (TIK), ETH Zürich
ETH Zentrum, 8092 Zürich, Switzerland
Tel: +41 1 632 70 05
Fax: +41 1 632 10 35
mwa@tik.ee.ethz.ch
http://www.tik.ee.ethz.ch/~mwa/

C
1024

0F D4 F7 A5 : D2 3D 85 43 : : 00 B3 03 D2 : 62 52 30 03

Rich Wales
California, USA
richw@webcom.com
http://www.webcom.com/richw/

C
1024

F2 9C 90 E0 : F3 B7 71 EC : : BC C1 B9 25 : 5E B3 9D FA

Leland A. Wallace
Apple Computer Inc.
1 Infinite Loop, Cupertino, CA 95014-6201, USA
randall@apple.com

C
1024

FE 06 6F F7 : 76 69 52 72 : : 3A 40 9F CF : 0A C4 F4 4A

Hans Wallberg
UMDAC - University of Umea
SE-901 87 Umea, Sweden
Tel: +46 90 786 5645
Fax: +46 90 786 6762
Hans.Wallberg@umdac.umu.se
http://poseidon.umdc.umu.se/

C
1024

2E C5 BB B7 : 82 46 B5 04 : : C3 C4 D8 8F : 07 39 CA 63

Peter N. Wan
College of Computing, Georgia Institute of Technology
P.O. Box 19679, Atlanta, Georgia, 30325-0679,USA
peter.wan@cc.gatech.edu
http://www.cc.gatech.edu/staff/w/Peter.Wan/index.html

B
1024

17 7A 7D D5 : 44 6B 66 10 : : 70 C0 CB 30 : 27 B1 1C 83

Andrew Watson
Object Management Group
492 Old Connecticut Path, Framingham, MA 01701, USA
Tel: +1 508 820 4300
Fax: +1 508 820 4303
andrew@omg.org
http://www.omg.org/~andrew

D
1024

EF FE 0C 30 : FF AD 34 F6 : : 33 33 5D FB : 94 75 2A 59

Stephen A. Weeber
weeber@mci.net
E6 E4 0B 79 : 9E 12 6E 7D : : 5F D0 B9 92 : A8 AB E1 7C
C 1024

Brian E. Weis
Cisco Systems
170 West Tasman Drive, San Jose, CA 95134-1706, USA
Tel: +1 408 526 4796
Fax: +1 408 526 4952
bew@cisco.com
19 26 0D 59 : 0C EA EC 99 : : BF 0E 60 DF : F2 38 F1 CB
C 1024

Petri Wessman
Petri.Wessman@hut.fi
http://www.akumiitti.fi/~orava/
3D D2 73 B8 : 0B B3 20 73 : : C1 80 FB 32 : 95 51 DD 6E
C 1024

Assar Westerlund
Swedish Institute of Computer Science
Box 1263, S-164 29 Kista, Sweden
assar@sics.se
http://www.sics.se/~assar/
85 E9 B4 8F : 95 63 F4 84 : : 96 71 C4 93 : 8D 6D 85 8D
C 1024

Michael Westlund
Royal Institute of Technology (KTH)
IT Advisory Board, SE-100 44 Stockholm, Sweden
westlund@admin.kth.se
http://www.admin.kth.se/~westlund/
AF 4E C9 49 : B4 AE 95 EA : : 03 18 FD 3F : E7 97 9E 7B
C 1024

Alan Westrope
awestrop@nyx.net
http://www.nyx.net/~awestrop
D6 89 74 03 : 77 C8 2D 43 : : 7C CA 6D 57 : 29 25 69 23
C 1024

Alan Wexelblat
wex@tinbergen.media.mit.edu
4D 38 84 BA : 25 D6 C0 08 : : 72 9D F8 7B : C3 00 1E 74
C 1024

Allen Wheelwright
D. E. Shaw Securities International
17 St Bedes Gardens, Cambridge CB1 3UF, United Kingdom
Tel: +44 976 612626
apwheelwright@iee.org
http://www.neosaur.demon.co.uk/allen
53 F1 AB 08 : B1 3D 5C 28 : : D2 AE CA 91 : CE 87 B4 C1
C 2048

Michael C. Whitman
Reston, Virginia USA
Tel: +1 703 689 6434
mike@sprint.net
http://whitman.sprintlink.net/~mike/
35 04 0F 59 : 56 08 AF 79 : : E3 D2 6F B0 : 82 13 8E DF
C 1024

Koerdien van Wijk
National Aerospace Lab.
Voorsterweg 31, 8316 PR Marknesse, The Netherlands
Tel: +31 527 248420
Fax: +31 527 248210
koerdien@nlr.nl
F6 02 BD AF : 6C 9F D2 80 : : A6 28 9E 03 : 40 FC 8E 54
C 1024

John Wilder
jwilder@llnl.gov
C9 5F A2 48 : B4 44 CD 3A : : A7 AA 55 26 : 21 B5 6A 9D
C 2048

Lars Wirzenius
liw@iki.fi
http://www.iki.fi/liw/
E7 FA 89 85 : 6D 9B 78 1D : : F5 30 EB FB : D8 11 CA 3F
C 1024

Thomas Witt
bach@polizei.net
69 E2 8E 25 : BC 89 CE FD : : C8 D6 E9 44 : 6E 1A 1B 3B
C 1024

Jeff Wolfe
wolfe@ems.psu.edu
5A DA 50 EC : EC 3D CB 05 : : 37 CD 96 84 : BC BC E2 EB
C 1024

Rob S. Wolfram
rwolfram@wi.leidenuniv.nl
http://www.mcs.nl/~rsw
31 09 D2 D7 : 57 B4 F4 FC : : CA FC 1F 34 : 8C BA C8 56
C 768

Alexander O. Yuriev
2024 Spruce Street, Suite 4, Philadelphia, PA 19103, USA
alex@yuriev.com
http://www.yuriev.com/People/Alex/
AE 84 53 43 : 77 CC C4 E2 : : 37 B1 3C 4D : 8C D3 D5 01
C 1024

Mario Zagar
Faculty of Electrical Engineering and Computing (FER)
Unska 3, 10000 Zagreb, Croatia
mario.zagar@fer.hr
http://www.rasip.fer.hr/mario
C
85 C0 CA F8 : 4E 49 D2 8B : : 9A 99 3A 1B : C6 2B FF 12 2048

Timothy S. Zakamaldin
Internet center, Novosibirsk State University
Russia
tim@uic.nsu.ru
http://www.it.nsc.ru/~tim
C
C3 D9 96 14 : BD 07 13 8F : : 14 9C 30 EF : 5C AA 75 F8 1024

Stefan Zehl
Simmernstr. 11, 80804 München, Germany
Tel: +49 177 2340515
Fax: +49 89 3618023
sec@42.org
http://www.42.org/~sec/
C
8E B4 17 47 : 33 64 E5 82 : : 01 6E DA EA : F7 EC A5 7D 2048

Erik Zeitler
Biology Education Centre, Uppsala University
Sweden
zeitler@ibg.uu.se
http://www.ibg.uu.se/~zeitler
C
45 CC 1B B7 : A3 36 90 A5 : : 70 4F EC A1 : F8 CE 03 4E 1024

Gideon Zenz
gzenz@ixc.net
C
EF EE 74 4B : 01 CE E0 D5 : : 6D DA E7 65 : E3 9C D3 6E 1024

Philip R. Zimmermann
prz@acm.org
A
9E 94 45 13 : 39 83 5F 70 : : 7B E7 D8 ED : C4 BE 5A A6 1024

Entrust/Solo Keys

Carlisle Adams
Entrust Technologies
Ottawa, Canada
carlisle.adams@entrust.com
http://www.entrust.com/
JMMP-GLHO-5LSE

A
S:27 Nov 2000
E:07 Oct 1998

Iain E. Buchan
Centre for Clinical Informatics
University of Cambridge, Institute of Public Health
Cambridge CB2 2SR, United Kingdom
Tel: +44 1223 330305
Fax: +44 1223 330330
ieb21@cam.ac.uk
http://www.medinfo.cam.ac.uk/personal/ieb/
NKCU-ASQL-CQZD

A
S:26 Jan 2001
E:26 Jan 2001

Mike Just
School of Computer Science, Carleton University
Ottawa, Ontario K1S 5B6, Canada
just@scs.carleton.ca
http://www.scs.carleton.ca/~just/
VO8Q-CX35-79W9

A
E:26 Nov 2000

Jong-Hyeon Lee
University of Cambridge, Computer Laboratory
Pembroke Street, Cambridge CB2 3QG, United Kingdom
Tel: +44 1223 334719
Fax: +44 1223 334678
jong-hyeon.lee@cl.cam.ac.uk
http://www.cl.cam.ac.uk/~jhl21
3LBU-EYTU-0JG9

A
S:26 Jan 2001
E:26 Jan 2001

Václav Matyáš Jr.
University of Cambridge, Computer Laboratory
Pembroke Street, Cambridge CB2 3QG, United Kingdom
Tel: +44 1223 334719
Fax: +44 1223 334678
vaclav.matyas@cl.cam.ac.uk
http://www.cl.cam.ac.uk/~vm206
EEMY-FRCA-YGHO

A
S:24 Nov 2000
E:24 Nov 2000

Tim Moses
Entrust Technologies
Ottawa, Canada
tim.moses@entrust.com
http://www.entrust.com/
EGCA-MEAB-H9VC

A
S:24 Feb 2001
E:7 Oct 1998

Fabien A.P. Petitcolas
University of Cambridge, Computer Laboratory
Pembroke Street, Cambridge CB2 3QG, United Kingdom
Tel: +44 1223 334676
Fax: +44 1223 334678
fabien.petitcolas@cl.cam.ac.uk
http://www.cl.cam.ac.uk/~fapp2
YHLF-RBET-DBD9

A
S:4 Feb 2001
E:4 Feb 2001

Paul C. Van Oorschot
Entrust Technologies
Ottawa, Canada
paulv@entrust.com
http://www.entrust.com/
QTSO-YVJK-3GR8

A
S:1 Nov 2000
E:7 Oct 1998

Michael Wiener
Entrust Technologies
Ottawa, Canada
michael.wiener@entrust.com
http://www.entrust.com/
94ND-BCKP-8VWR

A
S:27 Nov 2000
E:7 Oct 1998

Robert Zuccherato
Entrust Technologies
Ottawa, Canada
robert.zuccherato@entrust.com
http://www.entrust.com/
5VJK-CMLG-4XH3

B
S:22 Feb 2000
E:06 May 1999

8 Medical Keys

In this section, we include a number of keys used by medical practitioners in the UK. This section is experimental; it supports a number of exercises and pilots in which various organisations are trying to secure medical telematics applications. It contains one X.509 key and eight PGP keys. We expect that in the medium term it will expand; in the long term, books of medical keys may be issued separately (just as doctors' names, qualifications and so on are currently available in publications such as the Medical Register and the Medical Directory). Nonetheless, the Global Trust Register should contain top level keys for doctors, lawyers and other professions, as well as for commerce, industry, academia and government.

X509 Certificates

Clinical PET Centre
Guy's and St Thomas' Hospital
Lambeth Palace Rd
SE1 7EH London, United Kingdom
Tel: +44 171 922 8106
http://www-pet.umds.ac.uk

A
31 Dec 1999

2B C4 B7 81 : FD 92 B1 28 : : 4C 1B B4 8C : 80 A7 75 97

PGP Keys

William Beeby
Teeside encryption pilot
122 Hollowfield, Coulby Newham, Middlesbrough
Tel: +44 1642 598401
Fax: +44 1642 270055
william.beeby@onyxnet.co.uk
william.beeby@beeby.tees-ha.northy.nhs.uk

A
768

50 BB C2 58 : D3 8C 92 1D : : A3 66 E0 D4 : 4D 05 54 AC

Alan Hassey
Fisher Medical Centre
Skipton, N. Yorks, United Kingdom
alan_hassey@msn.com

A
1024

40 D9 32 4D : 86 D4 33 F1 : : 8A 77 3E 38 : 6B 70 56 A2

Grant Kelly
IT Chair, General Medical Services Committee
British Medical Association
Surgery: 8 Lavant Road, Chichester, West Sussex PO19 4RH, United Kingdom
Tel: +44 1243 527264
gkelly@enterprise.net

A 1024
47 E1 9C C0 : 3A 0B 59 19 : : 65 EA 64 DA : 7B 95 73 63

Ian Purves
University of Newcastle
ian.purves@newcastle.ac.uk

A 768
D0 2E 69 3D : EF 1D 5D DF : : 97 53 9F ED : BD 14 CF 06

Jane Rowlands
BMA Library, British Medical Association
Tavistock Square, London WC1H 9JP, United Kingdom
Jane@rowlands.demon.co.uk

A 1024
F6 8B 11 D9 : 0E BD 77 D3 : : 24 7C 74 06 : D6 54 28 CD

Sowerby Unit Key Server
Sowerby Unit for Primary Care Informatics
University of Newcastle
http://www.ncl.ac.uk/~nphcare/Sowerby/homepage.html

A 768
8F C6 ED 57 : 8C 01 E9 25 : : 11 3F 6D 31 : 60 1D B8 9F

Paul Steventon
Doctors' Independent Network
pauls@dinboard.demon.co.uk

A 1024
C0 94 AE 29 : 1E 8A 4B AB : : 18 91 C1 CE : C4 2D 2F 1C

John G. Williams
GP-Provider Links Project
St Luke's Surgery, Warren Road
Guildford, Surrey, United Kingdom
Tel: +44 1483 572364
Fax: +44 1483 440928
johnwill@bcsphcsg.demon.co.uk

A 1024
DB 68 70 F8 : B0 AF EA 70 : : ED 73 73 A8 : D8 FA DE 5E

9 Remailers

Finally, we include here some remailer keys. The procedure we adopted in selecting these keys was to send a test message to all the remailer addresses found in the MIT keyring, encrypted under the corresponding public key, and include those whose owners correctly decrypted and forwarded a message. This test was performed as close as possible to publication, in the last week of January 1998.

We have no knowledge of the principals behind these remailers and cannot, for example, guarantee that any particular remailer on this list is not transparent to the intelligence service of any particular country.

In general trust issues relating to anonymous remailers (and similar services such as anonymous web proxies) are less well understood than the corresponding issues for signature key certification. We hope that this situation may be clarified by further research and practical experience; in the meantime we award no trust rating to these keys.

EFGA Remailer List Signing Key
Electronic Frontiers Georgia
rlist@anon.efga.org
http://anon.efga.org/anon
6B F0 94 2D : 36 5A 7A 3E : : E9 90 7B A9 : A5 0D 45 8D 1024

Georgia Cracker Anonymous Remailer
Electronic Frontiers Georgia
remailer@anon.efga.org
http://anon.efga.org/anon
AB CB C1 43 : 89 91 DC 1A : : F2 09 28 39 : 2F 2D 5A E1 1024

LCS Remailer Administrator Key
MIT/LCS
mix-admin@anon.lcs.mit.edu
49 E1 1A B4 : 26 FD 81 2C : : CD B7 E7 47 : A7 0D 47 71 1024

Mixmaster Remailer (MIX)
mixmaster@remail.obscura.com
36 81 4B 3E : 26 3E 93 11 : : F8 61 4C DC : 42 BF 69 58 768

Quarter Horse
remailer@replay.com
31 3E E2 29 : 65 B6 17 76 : : CE E2 75 DD : 42 10 59 48 1024

Replay Remailer Service
remailer@replay.com
10 51 CD 21 : 7E C3 AC 69 : : 34 1F F0 04 : 62 EA 0D 33 1024

Shinobi Remailer
remailer@shinobi.alias.net
http://www.ee.siue.edu/~avankla/mix.help.html
9A 63 F3 0D : C1 7E A1 FA : : 02 BA F6 24 : D6 8E B5 89 1024

Squirrel Remailer
mix@squirrel.owl.de
3B A7 E3 AA : 82 76 DB 5E : : F3 CB 1C 9A : AA 4B 0F 80 1024