Global Secure E-mail Interoperability — The Europe-based Bridge-CA initiative

Bernhard Esslinger[1] · Detlef Hühnlein[2]

[1]Deutsche Bank AG
Breitlacherstraße 94, D-60489 Frankfurt, Germany
bernhard.esslinger@db.com

[2]secunet Security Networks AG
Sudetenstraße 16, D-96247 Michelau, Germany
detlef.huehnlein@secunet.com

Abstract

This paper provides an overview of the Europe-based Bridge-CA initiative, which aims at bridging the trust gaps between existing and emerging Public-Key Infrastructures of independent (corporate and government) organisations and hence allows secure transactions, such as e-mail-communication, *across* organisational boundaries.

1 Introduction

In view of the continuously growing electronification of business processes and utilisation of certificate-based applications in e-commerce, e-business and e-government, it becomes more and more important to design and implement inter-organisational Public-Key Infrastructures (PKI), which can be used to secure e-mail communication for example. While in a variety of groups of interest or enterprises there are already many isolated PKI-solutions in operation, or at least in construction, there seems to be a lack of possibilities to bridge the gap between these islands of trust. With this motivation Deutsche Bank AG, Deutsche Telekom AG and TeleTrusT e.V. started the Bridge-CA (B-CA) initiative, which aims at bridging the trust gaps between existing and emerging PKIs in order to allow secure transactions, such as e-mail-communication, *across* organisational boundaries. The B-CA board consists of Deutsche Bank AG, Deutsche Telekom AG, Daimler-Chrysler AG, SKO (Association of the German Savings Banks), TeleTrusT e.V. and BSI (German Information Security Agency). The current list of participating members, which passed the interoperability tests, comprises BMW AG, Dresdner Bank AG, Secartis AG, Siemens AG and TC TrustCenter GmbH for example and further participants from the private and public sector are explicitly solicited.

This paper provides an overview of the B-CA initiative, explaining its motivation and business considerations as well as technical issues of the current B-CA-implementation, including e-mail interoperability experiences, and plans for future development. This paper is organised as follows: Section 2 explains the basic motivation for this initiative and strategic business considerations. In Section 3, the basic design principles for the B-CA are stated. Section 4 sketches technical aspects of the current B-CA implementation, interoperability experiences

and future developments. Finally, Section 5 summarises the most important aspects of the B-CA initiative.

2 Motivation and strategic business considerations

In this section we will briefly explain the underlying motivation for the B-CA initiative and discuss strategic business aspects.

Today, more and more business processes in virtually all private and public organisations are supported, or even entirely performed, by electronic means. In most cases these processes handle valuable assets and hence it is important to provide adequate security mechanisms to protect these business processes. In most cases the implemented security mechanisms apply X.509 **[X.509]** certificates and hence it has been necessary to design and implement Public-Key Infrastructures (PKI) to manage the credentials used for encryption, authentication-services and digital signatures. However, apart from highly regulated (e.g. initiated by public authorities) or vendor driven infrastructures (e.g. by VeriSign, Entrust or RSA) most of these PKIs evolved in an independent manner and hence there are currently many different isolated corporate certificate hierarchies. Thus, even if most PKIs out there provide a similar level of trust and hence there should be no compelling reason, why these infrastructures should remain isolated, there has not been a general solution which bridges the gap between these „islands of trust“ in private and public (European[1]) organisations. The B-CA-initiative precisely aims at solving this problem by defining *minimum policy requirements* and *technical prerequisites* to allow secure transactions, such as e-mail communication, across organisational boundaries.

Gelöscht: legally binding

To understand the strategic importance of this approach we will answer the following simple questions:

- *Why is it important for organisations to extend their effective trust domain?*

  This is just because most business processes do not stop at the organisational border. Moreover, in the view of e-commerce, the external interfaces are obviously essential.

- *Why not just providing certificates within my hierarchy to customers, suppliers and partners?*

  Many parties are already using their own certificates and hence it would be neither sensible nor – when talking about high volumes – feasible to do this. OK, so one could simply consider foreign roots as trusted and have cross-certifications between the involved organisations.

- *Why joining the B-CA and not just cross-certifying with each partnering organisation?*

  The answer is very simple. This is explained by Metcalf's Law[2], which tremendous power can be seen from the development of the internet itself, which started in small military and academic communities and now is essential to virtually all organisations. Metcalf's Law means that the „value“ of a network is proportional to the square of the

-

[1] It should be noted, that a similar problem within the US-government area has been solved with the FB-CA-initiative **[NIST00]**, **[PoHa00]**. While the current B-CA is based in Europe, also non-European participants are explicitly solicited.

[2] Named after the former CEO of 3COM Corp.

number of nodes. And hence joining the B-CA-initiative via one simple cross-certification connects your organisation to a fast growing network, which helps your e-commerce and PKI-initiatives to reach the critical mass much faster.

Hence, the strategic importance of joining the B-CA-initiative may be summarised as follows:

Joining the B-CA-initiative helps to secure your investment

in PKI and e-commerce technology.

3 Design principles

From the brief discussion above, we will extract the main design principles for the B-CA-initiative.

- **Smooth integration**

  As there are already many isolated PKIs in operation, it is important that these PKI-solutions smoothly integrate with the B-CA. Therefore it is important, that the B-CA extends, and does not replace, existing organisational PKIs. Furthermore the B-CA should be based on internationally acknowledged standards, such as X.509 **[X.509]**, PKIX **[RFC2459]**, X.500 **[X.500]**, LDAP **[RFC2559]**, **[RFC2587]** and S/MIMEv2 **[RFC2311]**, **[RFC2312]** for example. This issue is important to avoid major changes to the existing PKIs and allow interoperability. Support of standards is clearly necessary for interoperability, but sometimes not sufficient. Therefore the B-CA will provide means to allow easy "real world" interoperability tests.

- **No inadequate regulatory burdens**

  While in some circumstances, it is important to provide and utilise a regulated framework for legally binding signatures and certificates, most of today's e-mail-based transactions do not require this very high level of trust and assurance. Therefore the B-CA initiative also aims at a lower level of trust, which only requires minimum policy and technical standards.

- **Scalability**

  As explained above, it is – for the sake of reaching a critical mass of participants - important that the B-CA is able to handle very many participating organisations from different countries. Furthermore it is important that the joining of new participants does not cause (much) additional effort for other participants. Finally, the B-CA should be able to work together with similar interoperability and trust initiatives all over the world.

- **Automated Processes**

  The targeted dimension also implies, that the processes for the B-CA-processor and the participating organisations are able to be performed in an automated manner. This means for example, that in long term perspective it is not tolerable that trust relationships have to be managed manually in de-central client systems.

- **80:20-principle**

  The "80:20-principle" means, that it takes 20% of the effort to reach 80% of the overall goals and the other 80% to approach the optimal solution (100%), which might never be reached entirely. Therefore it is advisable to be satisfied with a solution which only covers the most important aspects. This is especially important, if it is important to approach the market in a timely fashion.

4 Implementation aspects

In this section we will provide a brief overview of the most important aspects of the B-CA-implementation.

This section is structured as follows: In section 4.1 we will briefly highlight some aspects of the current B-CA implementation. In section 4.2 we discuss an open issue of the current implementation, describe the long term perspective of the B-CA and sketch a migration step for the B-CA and the participating organisations.

4.1 Current B-CA implementation

In this section we will provide a brief overview of the current B-CA implementation and highlight the necessary tasks for a participating organisation. Please refer to **[BCA01-b]** for more information on the necessary technical steps to participate in the B-CA initiative.

As described in **[BCA01]**, participating in the B-CA initiative makes the following simple steps necessary:

- Policy examination
- Contact
- Interoperability test
- Contract conclusion
- Use

4.1.1 Policy examination

The first step for a prospective participant who wants to join the B-CA initiative is to check, whether its PKI meets the minimum requirements as defined by the B-CA board. The minimum requirements, as sketched in **[BCA01-a]**, are as follows:

- **Policy requirements**
  - Personal identification and registration of the certificate holder

    In order to guarantee the binding between a public key and a person, it is required to perform personal identification and registration of the certificate holder. Bulk registration is only admissible, if the respective data sources are sufficiently trustworthy.

- Availability of certificate status information via CRLs or OCSP

  Certificate status information must be made available for the B-CA as well as its participants. Note, that in some environments the access to the corporate directory, or to an OCSP-responder, across the corporate firewall might be in conflict with corporate security policies.

- Unique Distinguished Names

  The Distinguished Names in the certificates must be uniquely assigned and may not be in conflict with name spaces from other participating organisations. This is especially important for future B-CA developments which will involve cross-certification and (optional) directory chaining.

- RSA key length of at least 1024 bit
- Key Usage is "Signature" and/or "Encryption"

- **Interoperability requirements**

  Please refer to Section 4.1.3 for interoperability requirements.

4.1.2 Contact

As soon as the basic policy check is performed, the prospective participant may get in contact with the B-CA executives. A contact form and further contact information is available at **[BCA01]**.

4.1.3 Interoperability test

The next major step is to perform suitable interoperability tests with the B-CA. This process is assisted by B-CA staff members and typically takes very little effort. This section is structured as follows. Section 4.1.3.1 lists the interoperability requirements. Section 4.1.3.2 provides the most important findings of the interoperability tests performed by the B-CA.

4.1.3.1 Interoperability requirements

The minimum interoperability requirements for joining the B-CA initiative are as follows:

- X.509v3 Certificates, as defined in **[X.509]**
- As few as possible critical extensions in certificates

  It is recommended to use a similar profile as defined in PKIX **[RFC2459]**.

- The certificates must be available in standard formats, like .crt, .der or .p7c
- The e-mail-client must be able to
  - import root certificates (in standard formats, like **[PKCS7]** for example)

- support the S/MIMEv2 **[RFC2311]**

  If the client software only supports a subset of the S/MIMEv2 signature formats, the support of *single-signed-opaque* messages is mandatory, while the support of multi-part-signed-cleartext is optional.

If a sub-tree of an existing PKI wishes to participate in the B-CA initiative, it is important that the fields “Subject Key Identifier” and “Authority Key Identifier” are *not* set in order to allow multiple super-ordinate certificates.

While the following features are not strictly required for participating in the B-CA initiative, they should be supported if participants wish to support future B-CA developments, like cross-certification.

- The CA-software should be able to issue PKCS#10 **[PKCS10]** certification requests to the B-CA
- The participants directory should be able to
  - handle attributes related to cross-certificates (see **[X.509]**, Section 8)
  - allow X.500 **[X.500]** chaining or suitable duplication mechanisms, like they are currently defined in the LDUP working group **[ApSt01]**.
- The e-mail clients should be able to handle LDAPv3 **[RFC2251]** referrals

  As discussed in **[NIST00]** and **[PoHa00]**, this requirement can be dropped, if X.500-compliant directories are used. Especially, as some of the participant's directories will not be X.500-compliant, it is important, that the e-mail-clients are able to handle LDAPv3 referrals for CRL retrieval. For this purpose NIST is working together with major client-vendors to resolve current deficiencies **[Burr01]**.

4.1.3.2 Interoperability experiences

The B-CA has performed basic e-mail interoperability tests with widely used client systems. The abstract results of this interoperability tests may be found in **[BCA01-c]**. Please refer to **[BaJH01]** for more details.

The client systems used in this test were:

- Lotus Notes 4.x (with Mailprotect PlugIn)
- Outlook 98 (with AuthentEmail PlugIn / SIKOM)
- Outlook 98 (native, with 128 Bit Patch)
- Outlook 2000
- Netscape Messenger

The tests can be summarised as follows:

- **Encryption and Signature**

  All tests were performed successfully.

- **Encryption only**

  Except from some cosmetic problems with the native version of MS Outlook 98, like lost icons and a new attachment "winmail.dat", all tests were performed successfully.

- **Signature only**

  Besides such cosmetic problems with MS Outlook 98, there have been other problems which are due to the fact that some of the tested e-mail clients only support a certain subset of S/MIMEv2 **[RFC2311]**. In particular Mailprotect for Lotus Notes 4.x only supports the message format single-signed-opaque, while Netscape only supports multipart-signed-cleartext. While there is a simple workaround for Lotus Notes to allow other clients to verify its signatures, signatures generated by Netscape's Messenger are not verifiable by Lotus Notes clients. In this scenario it is recommended to send messages signed and encrypted.

4.1.4 Contract conclusion

Next, the new participant will sign a contract of participation with the B-CA initiative and interchange its root certificate with that of the B-CA.

4.1.5 Use

As soon as the contact person, typically a PKI administrator, receives the signed list of root certificates from the B-CA, it will verify the signature on this list and – if ok – start with the internal distribution of the new list of trusted certificates. This local PKI administrator is responsible for the secure internal distribution of the trusted roots and the detailed steps, which are necessary to perform this task, are heavily depending on the applied systems and practices within the participating organisation.

While in some organisations, it will be possible to manage the trust relationships at a central place, there may be other organisations in which this central management is not (yet) possible. In this case the PKI administrator may want to store the (new) trusted roots on a secure internal web site, which may be accessed by the local clients or even need to put further efforts in the de-central configuration of the involved client systems.

This internal management obviously creates administrative problems for those participants, which are not (yet) able to manage this trust relationships at a central place. The solution for this problem is outlined in the next section.

4.2 Open issues, long term perspective of B-CA and migration steps

Section 4.2.1 briefly highlights an open issue of the current B-CA implementation. Section 4.2.2 explains the long term perspective for the B-CA and section 4.2.3 discusses a possible migration step.

4.2.1 Internal trust management - an open issue

Considering the current implementation, the obvious problem for some participating organisations is the internal management of the trusted root certificates. It is clear, that – on a long term basis – the local PKI administrators are not keen to configure every single local client.

Hence there must be some standardised way to manage the trust relations induced by the B-CA at a central place.

4.2.2 Long term perspective for B-CA architecture

This potential problem is solved by the long term goal of the B-CA, which aims at providing a (hub and spoke) cross-certified structure, similar to the Federal Bridge CA initiative in the US **[NIST00]**, **[PoHa00]**, which reduces the overall management tasks for enabling a new participant to simple operations performed by the B-CA administrators.

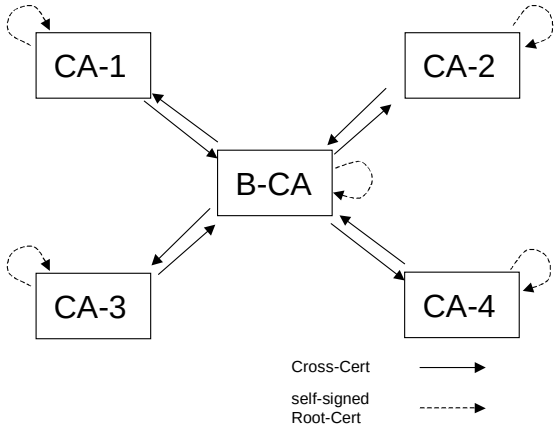

Figure 1: Hub and Spoke B-CA architecture

As shown in Figure 1, the B-CA will serve as central instance which will perform cross certifications with the participating CAs. Thus the entire management overhead for new participants is shifted to the B-CA instead of the participating organisations. Technically, this cross-certification will be performed by creating the corresponding cross certificates and storing it in the central bridge directory, as standardised in X.509 **[X.509]** (Section 8) and further profiled in RFC 2587 **[RFC2587]** for the LDAPv2[3]-environment:

```
crossCertificatePair ATTRIBUTE     ::={
     WITH SYNTAX                         CertificatePair
     EQUALITY MATCHING RULE              certificatePairExactMatch
     ID                                  id-at-crossCertificatePair },
```

where

```
CertificatePair                     ::=   SEQUENCE {
     forward     [0]                                  Certificate OPTIONAL,
     reverse     [1]                                  Certificate OPTIONAL
}.
```

In **[X.509]** it is standardised, that the **for**ward-certificate is the certificate which is issued **for** the corresponding CA. The reverse certificate is the certificate which is issued by the CA.

The relevant entries in the directories are shown in Figure 2.

-

[3]It should be noted, that LDAPv3 uses the same profile for handling cross-certificates.

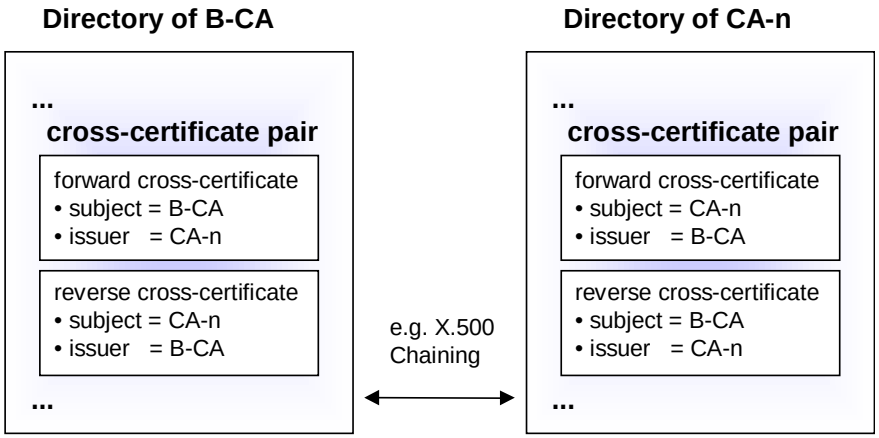

Figure 2: Directory entries

As shown in **[NIST00]**, this approach is indeed feasible, if X.500 directories are involved. However as many organisations do not apply X.500 directories, the e-mail clients will need to handle LDAPv3 referrals. Currently, most e-mail clients do not yet fully support this functionality. While it is possible to provide all certificates in the certification path attached to the message, the support of LDAPv3 referrals to retrieve CRLs, or equivalent online status information **[RFC2560]**, from different sources is subject to further development at the client-vendor's side.

Besides these developments there will be future developments at the B-CA which will define suitable profiles for the involved cross-certificates which will take into account constraints of the path-lengths and name-spaces as well as issues of policy mapping.

4.2.3 Unilateral cross-certification as possible migration step

As long as the B-CA is not entirely set up in the way outlined above, and as long the number of participating organisations is not too big, it might be advisable for participating organisations, which are able to handle cross certificates, to issue cross certificates for all roots, which are received by the PKI administrator. Hence the organisation should aim at enabling cross-certification at its own site, while the B-CA is being developed. This intermediate step will allow a smooth switch to the final B-CA structure, which basically consists of creating the cross certificates for the B-CA and then revoking all direct cross certificates.

5 Summary

As discussed in this paper, the B-CA provides simple means to bridge isolated islands of trust and allow secure business processes, like e-mail communication, across organisational boundaries. The B-CA activities also prove that basic S/MIME interoperability issues are sufficiently solved to allow secure e-mail transactions between different organisations - using systems from different vendors. The first experiences gathered in this project, as well as the outlined future paths, may serve as input for various organisations and system vendors to move towards a secure business world by enabling global secure e-mail interoperability.

References

[ApSt01] Apple, C.; Strassner, J.: *LDUP - LDAP Duplication/Replication/Update Protocols*, results of working group via

http://www.ietf.org/html.charters/ldup-charter.html

[BaJH01] Bartels, M.; Jaletzke, A.; Hühnlein, D.: *Bridge-CA – Basic S/MIME Interoperability*, (in German), 2001, available upon request from the present authors

[BCA01] Bridge-CA: *Web-site* at http://www.bridge-ca.org

[BCA01-a] Bridge-CA: Bridge-CA - Participation Requirements, via

http://www.bridge-ca.org

[BCA01-b] Bridge-CA: Bridge-CA - Participation Roadmap, via

http://www.bridge-ca.org

[BCA01-c] Bridge-CA: *Bridge-CA - Interoperability*, via http://www.bridge-ca.org

[Burr01] Burr, W. E., representative of the Federal Bridge Certification Authority, personal communication, 2001

[NIST00] NIST: Report of Federal Bridge Certification Authority Initiative and Demonstration – Electronic Messaging Association Challenge 2000, Draft 101500, 2000, via

http://csrc.nist.gov/pki/documents/emareport_20001015.pdf

[PKCS7] RSA Laboratories: *PKCS #7 - Cryptographic Message Syntax Standard*, via http://www.rsalabs.com/pkcs/pkcs-7/index.html

[PKCS10] RSA Laboratories (Kaliski, B.): PKCS#10 - Certification Request Syntax Standard, Version 1.5, RSA-Laboratories, via

http://www.rsalabs.com/pkcs/pkcs-10/index.html

[PoHa00] Polk, W.T.; Hastings, N.E. (NIST): Bridge Certification Authorities: Connecting B2B Public Key Infrastructures, via http://csrc.nist.gov/pki/documents/B2B-article.pdf

[RFC2251] Wahl, M.; Howes, T.; Kille, S.: *Lightweight Directory Access Protocol (v3)*, via http://www.ietf.org

[RFC2311] S. Dusse, P. Hoffman, B. Ramsdell, L. Lundblade, L. Repka: *S/MIME Version 2 Message Specification*, via http://www.ietf.org

[RFC2312] S. Dusse, P. Hoffman, B. Ramsdell, J. Weinstein: *S/MIME Version 2 Certificate Handling*, via http://www.ietf.org

[RFC2459] Housley, R.; Ford W.; Polk W. und Solo D.: *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, via http://www.ietf.org

[RFC2559] Boeyen, S.; Howes, T.; Richard P.: Internet X.509 Public Key Infrastructure Operational Protocols — LDAPv2, via http://www.ietf.org

[RFC2560] Myers, M., Ankney, R., Malpani, A., Galperin, S., Adams, C.: *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol*, via http://www.ietf.org

[RFC2587] Boeyen, S.; Howes, T.; Richard P.: *Internet X.509 Public Key Infrastructure LDAPv2 Schema*, , via http://www.ietf.org

[X.500] ITU-T Recommendation X.500: *The Directory—Overview of Concepts and Models*, International Telecommunication Union, Genf, Schweiz, 1997 (equivalent to ISO/IEC 9594-1)

[X.509] ITU-T Recommendation X.509: *Information Technology—Open Systems Interconnection—The Directory: Authentication Framework*, International Telecommunication Union, Genf, Schweiz, 1997 (equivalent to ISO/IEC 9594-8)