This document contains a brief overview of the technical capabilities of our Anonymous Credentials System on a NXP JCOP 41 v2.2 [4]. Further questions on anonymous credential systems can also be directed to idemix@zurich.ibm.com.

Basic Specification

We present an anonymous credential system on Java Card which supports sustainable secondary use of identity attributes. The system enables a strong combination of accountability and privacy.

Being an autonomous trust root, the system allows to anonymously proof possession of a certificate or disclosing selective attributes while keeping others completely confidential. Transactions of the system are completely unlinkable. However, certificates can be revoked by an authorized authority.

The system is based on the Camenisch-Lysyanskaya signature scheme [1], the Identity Mixer cryptographic library [3], and the TPM’s Direct Anonymous Attestation (DAA) [2].

Anonymous Credential System

System Properties

- Autonomy – All computation on card, secure against malicious terminals.
- Confidentiality – The user’s master key is retrained confidential throughout the card’s life-cycle.
- Unlinkability – All credential system transactions are fully unlinkable.
- Future-proofness – The credential system transactions are controlled by dynamic and versatile policies. Future proof key lengths are possible.
- Efficiency – The credential system has a pre-computation time of 7.5s and a user response time after policy consent of 2.5s using 1536-bit keys.

Card Setup

- User Master Key – The card holds a confidential master key that is never disclosed to any other party throughout the life-cycle.
- Issuer Entries – The credential system supports multiple (up to five) issuer entries.
- Certificate Entries – The credential system can host multiple (up to ten) certificate entries with up to ten attributes.
- Update – certificates can be removed and updated in trusted environments.
Proof of Possession
- The credential system proves in zero-knowledge that the card owns a valid certificate without disclosing any other information about the user. The transaction is fully unlinkable.
- The proof statement is an electronic signature that the verifier can validate against the public key of the issuer.

Selective Attribute Disclosure
- The credential system discloses selected attributes to the verifiers and proves the ownership of the corresponding valid certificate to the verifier.
- The proof statement is an electronic signature that the verifier can validate against the public key of the issuer.

Key Lengths and Transaction Times
The IDMX JCOP card supports multiple key lengths depending on the security and future-proof requirements of the overall system.

<table>
<thead>
<tr>
<th>Modulus</th>
<th>1280 bit</th>
<th>1536 bit</th>
<th>1984 bit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-computation</td>
<td>5203 ms</td>
<td>7828 ms</td>
<td>13250 ms</td>
</tr>
<tr>
<td>Blind certificate</td>
<td>2125 ms</td>
<td>2906 ms</td>
<td>5000 ms</td>
</tr>
<tr>
<td>Compute ZKPoK Commitment</td>
<td>3078 ms</td>
<td>4922 ms</td>
<td>8250 ms</td>
</tr>
<tr>
<td>Policy-dependent</td>
<td>2234 ms</td>
<td>2625 ms</td>
<td>3298 ms</td>
</tr>
<tr>
<td>Compute 1 ZKPoK Response</td>
<td>562 ms</td>
<td>656 ms</td>
<td>828 ms</td>
</tr>
<tr>
<td>Total</td>
<td>7437 ms</td>
<td>10453 ms</td>
<td>16548 ms</td>
</tr>
</tbody>
</table>

Optional Features
The standard operation mode of the credential system is to prove the possession of a certificate only, without including attributes in the actual cryptographic signature. Attribute statements are backed by the tamper-resistance of the JCOP card [4].

Attribute Signatures
- The credential system includes certified attributes in the certificate as well as proofs of possession and selective disclosures.
Each additional attribute costs additional 1684 ms transaction time at a modulus bit length of 1536 bits. Of this, 1016 ms are pre-computation; 668 ms are policy-dependent.

Anonymous Revocation (for v. 1.1)
- The credential system includes an anonymous revocation mechanism that allows authorities to revoke cards and verifiers to check a card’s validity. It is standardized as part of the TPM Direct Anonymous Attestation (DAA) [2].
- With a 1536-bit modulus, this makes an additional estimated transaction time of 1474 ms, which can be fully handled at pre-computation time.

Camenisch-Groß Attribute Encoding (for v. 1.1)
- The credential system encodes binary and finite-set attributes highly efficiently [7]. It includes these certified attributes in the certificate as well as proofs of possession and selective disclosures at a minimum overhead.
- This will add estimated 1684ms transaction time at a modulus bit length of 1536 bits. Of this, 1016 ms are pre-computation; 668ms are policy-dependent. Note that these are upper bounds for the full exponent length.

Coarse-Grained Interval Proofs (for v. 1.2)
- The credential system encodes attribute ranges of users (e.g., birthday) highly efficiently. A cryptographic range proof (e.g., current year - birth year > 18) based on certified values comes at a minimum overhead.
- This will add estimated 1684ms transaction time at a modulus bit length of 1536 bits. Of this, 1016 ms are pre-computation; 668ms are policy-dependent.

Technology Basis
We cite the following properties of the underlying JCOP platform from the JCOP30 Technical Brief [4].

JCOP 41 v2.2 Java Card
JCOP 41 v2.2 is a dual-interface member of the NXP JCOP family. It supports ISO7816 and ISO14443A (T=CL).
The platform was certified by the German Bundesamt für Sicherheit und Informationstechnik (BSI) for
- **Functionality:** product-specific security target (Common Criteria Part 2 ext)
- **Assurance:** Common Criteria Part 3 conformant, EAL 4 augmented with ADV_IMP.2, ALC_DVS.2 (under certification BSI-DSZ-CC-0294-2006 [6])

Communication
- **Supported Protocols:** ISO7816 T=1 direct convention [default], ISO7816 T=0 direct convention, ISO7816 T=1 inverse convention, ISO7816 T=0 inverse convention, ISO14443A T=CL.
Contact protocols: At the default clock rate of 3.57 MHz, the following speeds can be attained: 9600 bit/s [default], 19200 bit/s, 38400 bit/s, 57600 bit/s, 115200 bit/s.

Contactless protocol: 106000 bit/s, 212000 bit/s, 424000 bit/s, 848000 bit/s.

JCOP Features

- **Java Card Garbage Collection**: fully implemented
- **Java Card Cryptographic Algorithms**: JCOP has the ability to generate RSA keys on the card (following constants as known from the Java Card specification [5]).
- **Ciphers**: ALG_DES_CBC_NOPAD, ALG_DES_CBC_ISO9797_M1, ALG_DES_CBC_ISO9797_M2, ALG_DES_ECB_NOPAD, ALG_DES_ECB_ISO9797_M1, ALG_DES_ECB_ISO9797_M2, ALG_RSA_PKCS1, ALG_RSA_NOPAD.
- **Signatures**: ALG_DES_MAC8_NOPAD, ALG_DES_MAC8_ISO9797_M1, ALG_DES_MAC8_ISO9797_M2, ALG_RSA_SHA_ISO9796, ALG_RSA_SHA_PKCS1, ALG_RSA_MD5_PKCS1.
- **MessageDigest**: ALG_SHA, ALG_MD5.
- **RandomData**: ALG_SECURE_RANDOM.

Acknowledgements

We want to thank Patrik Bichsel and Jan Camenisch for their contributions and feedback to this document as well as the general line of work.

References


