<https://www.securetechalliance.org/resources/pdf/OPACITY_Overview%203.8.pdf>

OPACITY: Open Protocol for Access Control and Ticketing with PrivacY

Protocol suite for authentication and key agreement optimized for contactless transactions.

NIST SP 800-56A compliant.

Only one command/response pair

Relies on Elliptic Curve Cryptography ECDH/ECDSA, as well as AES and SHA256.

Supports 2 protocols:

* Zero Key management (ZKM aka SMAv3), doesn’t require any secrets stored on a terminal.
* Forward Secrecy (FS) requires static PKI credential stored on terminal, but enhanced privacy protection

Reference implementation provides Secure Authentication Module (SAM) applet/library. SAM is smartcard device embedder in the terminal. (For storing secrets)

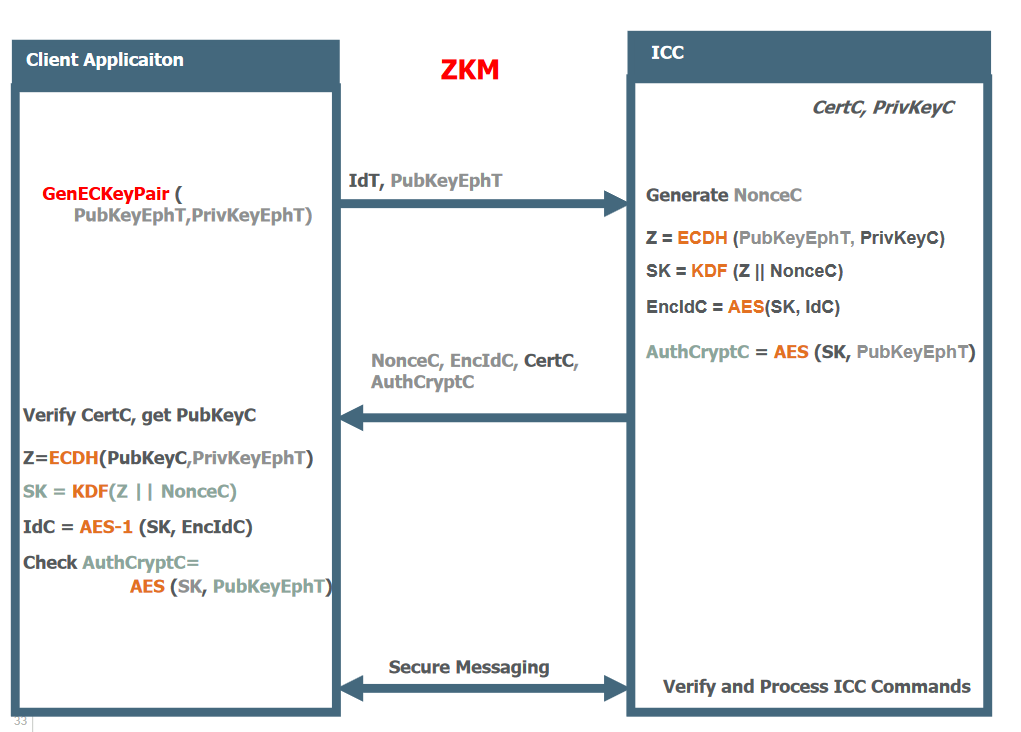
ZKM doesn’t require a SAM. Only requires root public key of CVC Digital Signatory to be protected by the terminal. (rather than MASTER and private keys). SAM could still be used to store public key.

SAM software library can never exceed fips140-2 level 1. Applet on specialised hardware can reach fips140-2 level 3.

SAM activation: SAM operations protected by an access control rule. Admin operations protected by GlobalPlatform secure channels. Usage is protected by PIN/OPACITY based auth by control panel to SAM. Policy-based deactivation of SAM makes it lose its state.

Go with ZKM.

Persistent Binding: pre-session keys cached by User applet and Terminal applet, allows for faster transactions for that user card next time.



PLAID:

<https://www.humanservices.gov.au/organisations/about-us/publications-and-resources/protocol-lightweight-authentication-identity-plaid>

Best not use it: <https://www.schneier.com/blog/archives/2015/10/weaknesses_in_t.html>

NIST 800-73-4:

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-73-4.pdf>

Some other protocol published 2004:

<https://link.springer.com/content/pdf/10.1007%2F1-4020-8143-X_23.pdf>

Points from the paper:

Previously the main prohibitor to smartcard public key cryptography was limited card processing power.

* [www.dice.ucl.ac.be/cascade](http://www.dice.ucl.ac.be/cascade)
* Generation of prime numbers or pairs for elliptic curves was slow in software.

Public key based architecture requires existence of public key infrastructure (PKI) [ISOIIEC 11770-3, "Information technology -- Security techniques – Key management -- Part 3: Mechanisms using asymmetrie techniques", ISO 1999]

Most public key cryptography secure channel protocols not specifically designed for smart cards. E.g. limited communication buffers usually between 190-255B so the number of messages exchanged should be minimal.

GlobalPlatform:

* Card specification. Provides functionality e.g. key management/storage etc.
* Secure multi-application card management.
* Closely coupled with Java Card technology (but no necessary dependency)
* Secure channel – mechanism allowing card and host to authenticate each other and establish session keys to protect subsequent communication. GlobalPlatform spec defines 2 protocols for this: SCP01 and SCP02. Both symmetric protocols.
* GlobalPlatform has Security Domains. On-card representative of card issuer or app provider. Allows issuers to share control over portion of the card with approved partners. Security domains also responsible for cryptographic functions and key handling

Note: FIPS140-2 is a US government security standard for cryptographic modules.