DCE RFC 68.4
Public Key Certificate-Based DCE Login

The Open Group Member's Meeting

27 April - 01 May 1998

San Diego, Calif. USA

Agenda

- Introduction and history
- Key technologies, standards
- Basic PK-INIT KRB_AS_REQ/REP flows
- Privilege Service changes
- The end-goal
- Proof-of-concept demo
- Qs&As

History

- Initial DCE Public Key work done in DCE 1.2.2.
  - PKI was immature, products/stds were evolving at this time.
- IETF PKINIT protocol specification moved on after DCE 1.2.2.
- SIMC catalyzed customer requirements for DCE-PKI integration.
- Vendors met to work on open architecture.

History *(continued)*

- DASCOM, Digital and IBM proposed a solution.
- IETF CAT Working group modifying PKINIT to support solution.
- TOG+vendor agreement with proposal, providing feedback.
- TOG Fast Track proposal now pending.

Motivations

- Some PKI based mechanisms are inevitable:
  - Signing of email messages
  - Non-repudiation enablement
  - Scaleable authentication for e-commerce applications
- Cross-organizational trust models for extranets
- Laymen's terms result of DCE-PKI integration:
  - ***If an email can be signed, a DCE login can be achieved via the same mechanism that signs the email***
- Integrated environment: Digital signatures & envelopes
- DCE's "role" is as an authorization system for PKI

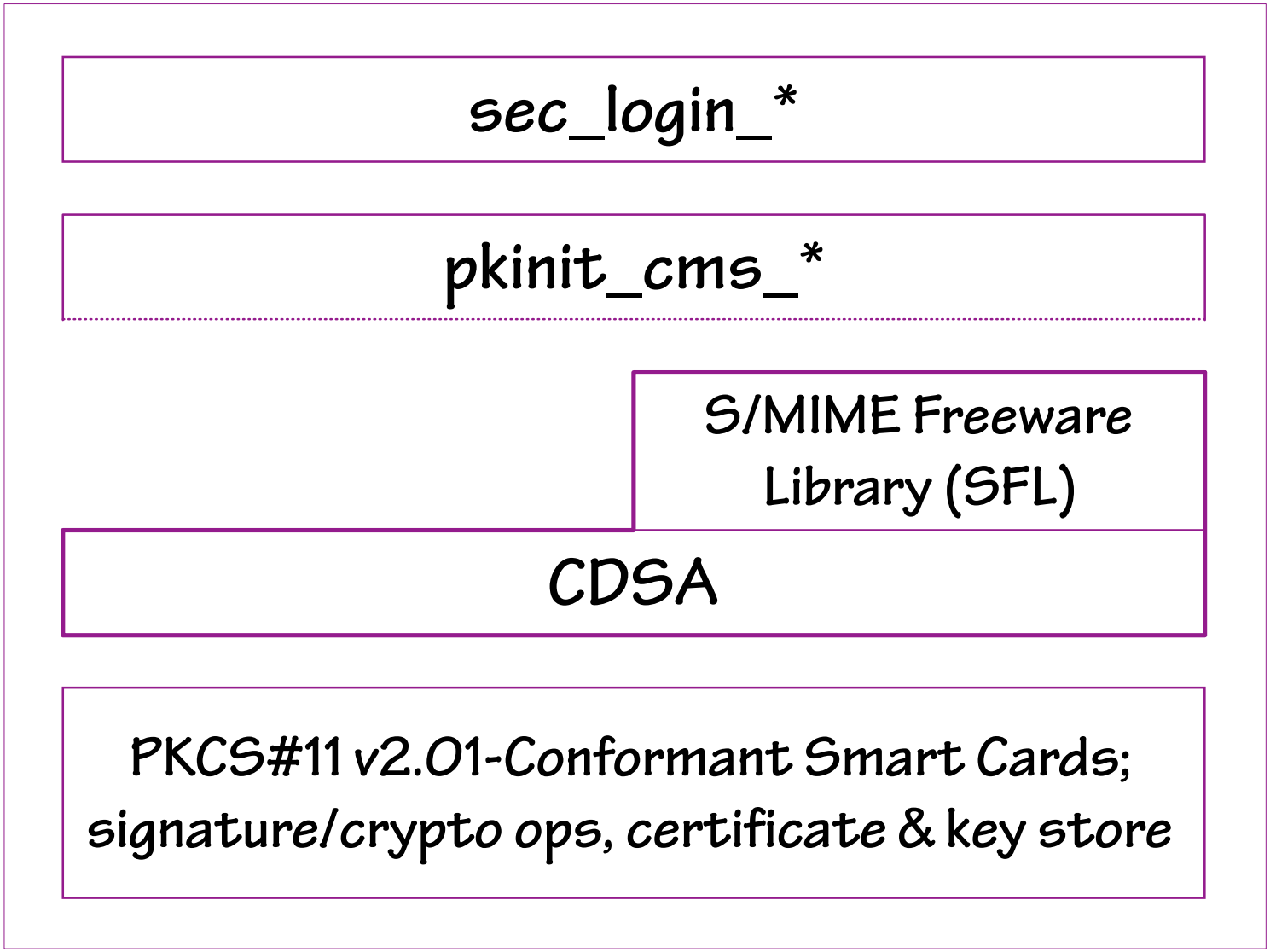
RFC 68.4 Synopsis

- X.509v3 Public Key Certificates for authentication to DCE
  - The DN is the principal
- New pkinit_cms_* component
  - Cryptographic Message Standard (CMS) for digitally signing and enveloping parts of Kerberos authentication flows
  - Isolation of the public key certificate and CMS functionality
  - Support for smart cards and delivery of a software smart card in the reference implementation
  - "PKI-neutral" implementation that supports multiple PKIs.
- A Credential Acquisition Service
  - Input: Verified DN
  - Output: EPAC
  - Enables an installation to implement its own DN==>EPAC mappings.

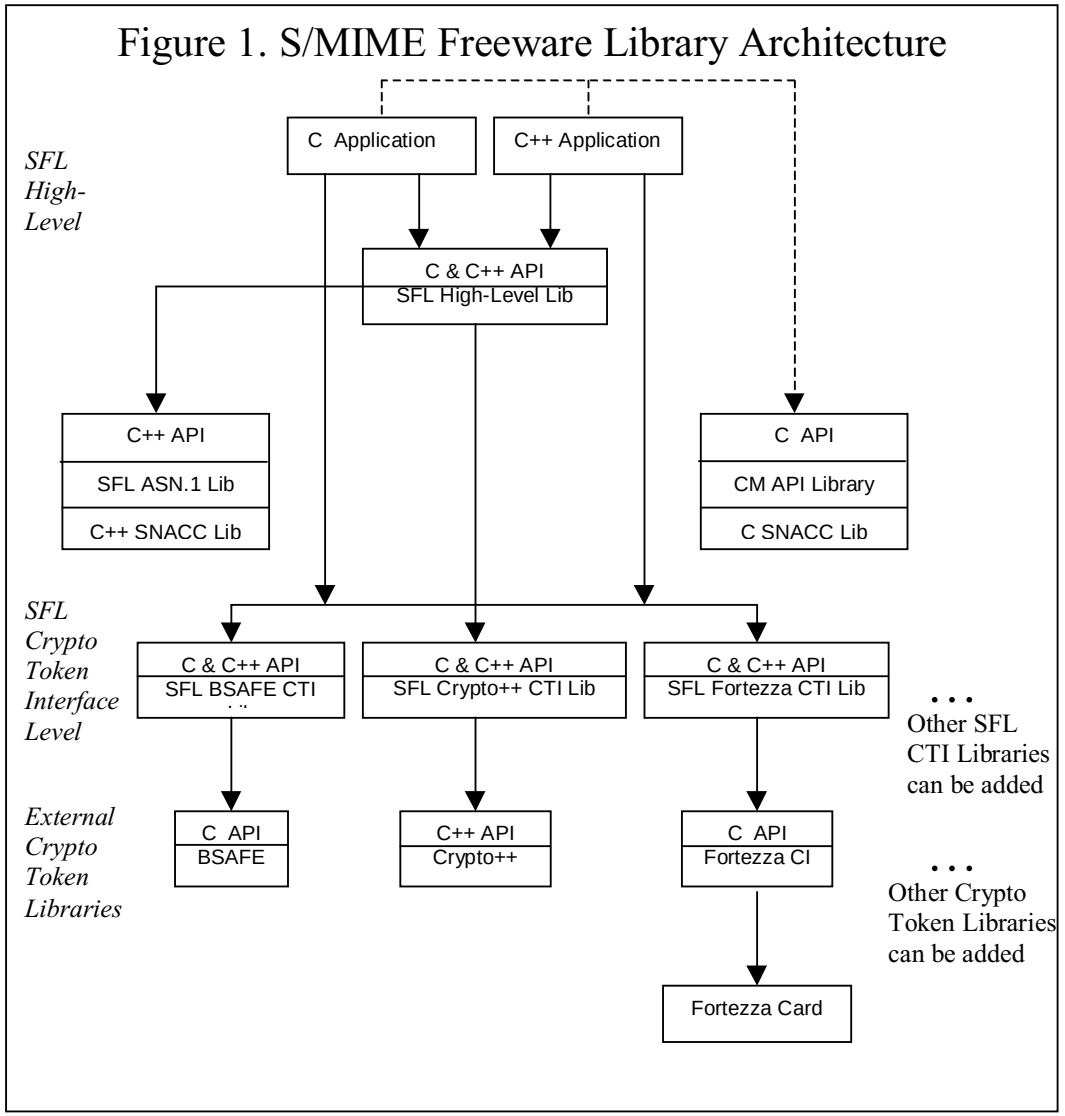
Architectural Foundation

- KRB_AS_REQ/REP Kerberos messages upgraded/rationalized to latest IETF "PK-INIT" Draft
- Cryptographic Message Syntax (CMS) used to create/consume signed and enveloped messages within the PK-PA-AS-REQ/REP PADATA portions of the KRB_* messages
- Reference implementation will use CDSA for low-level crypto, certificate/trust and data store operations

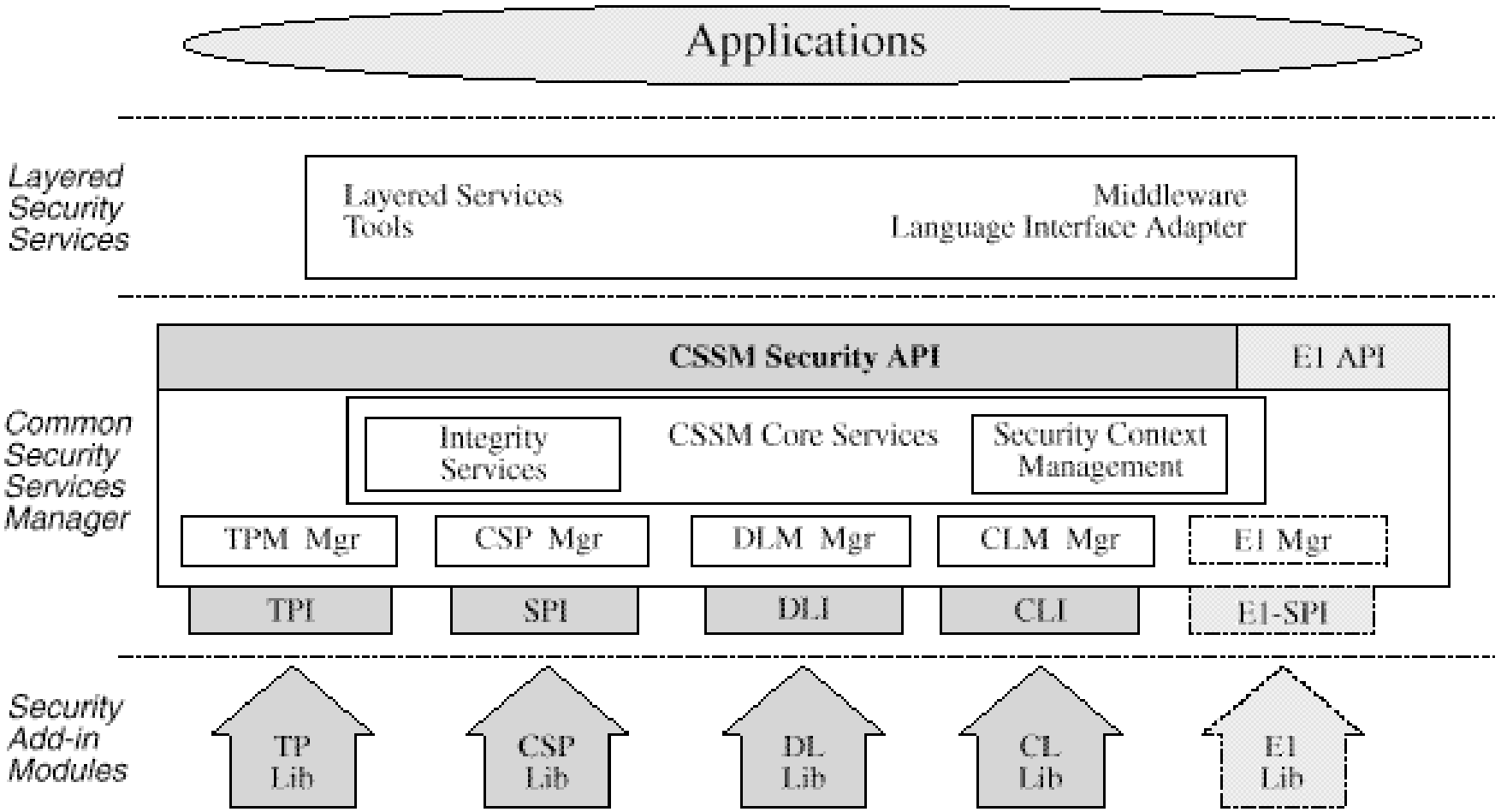
Architectural Foundation *(continued)*



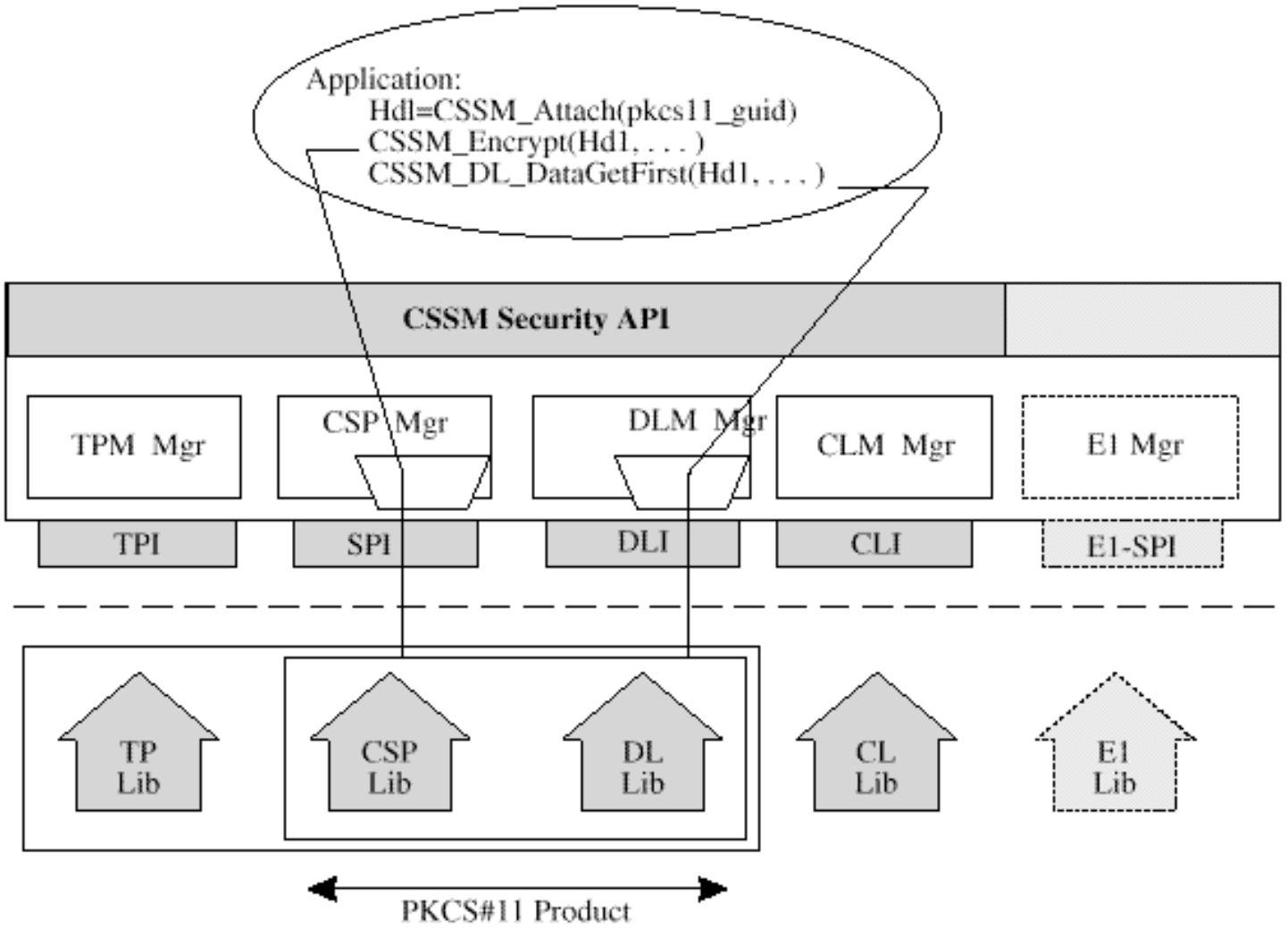
SFL Architecture



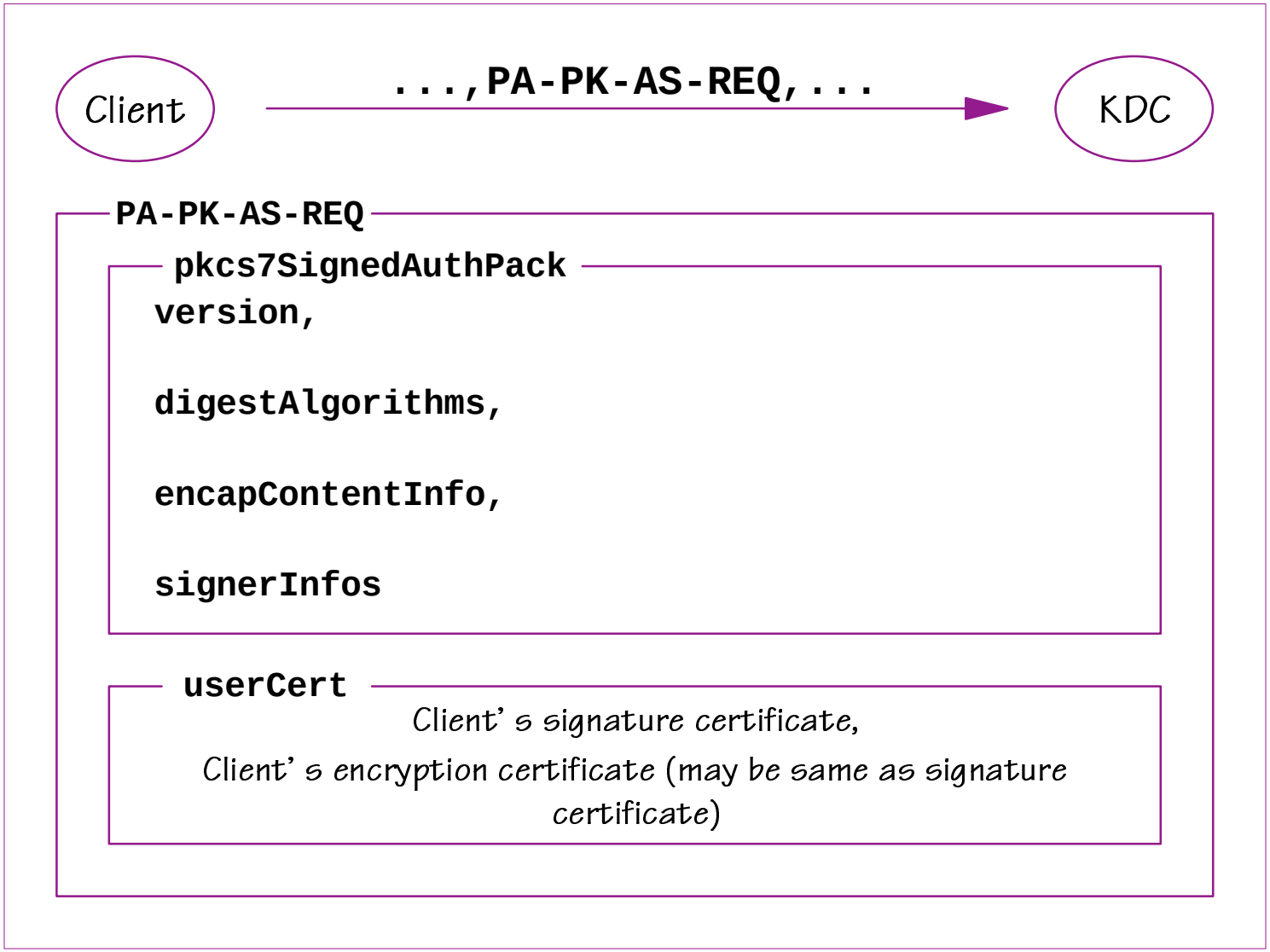
CDSA Overview



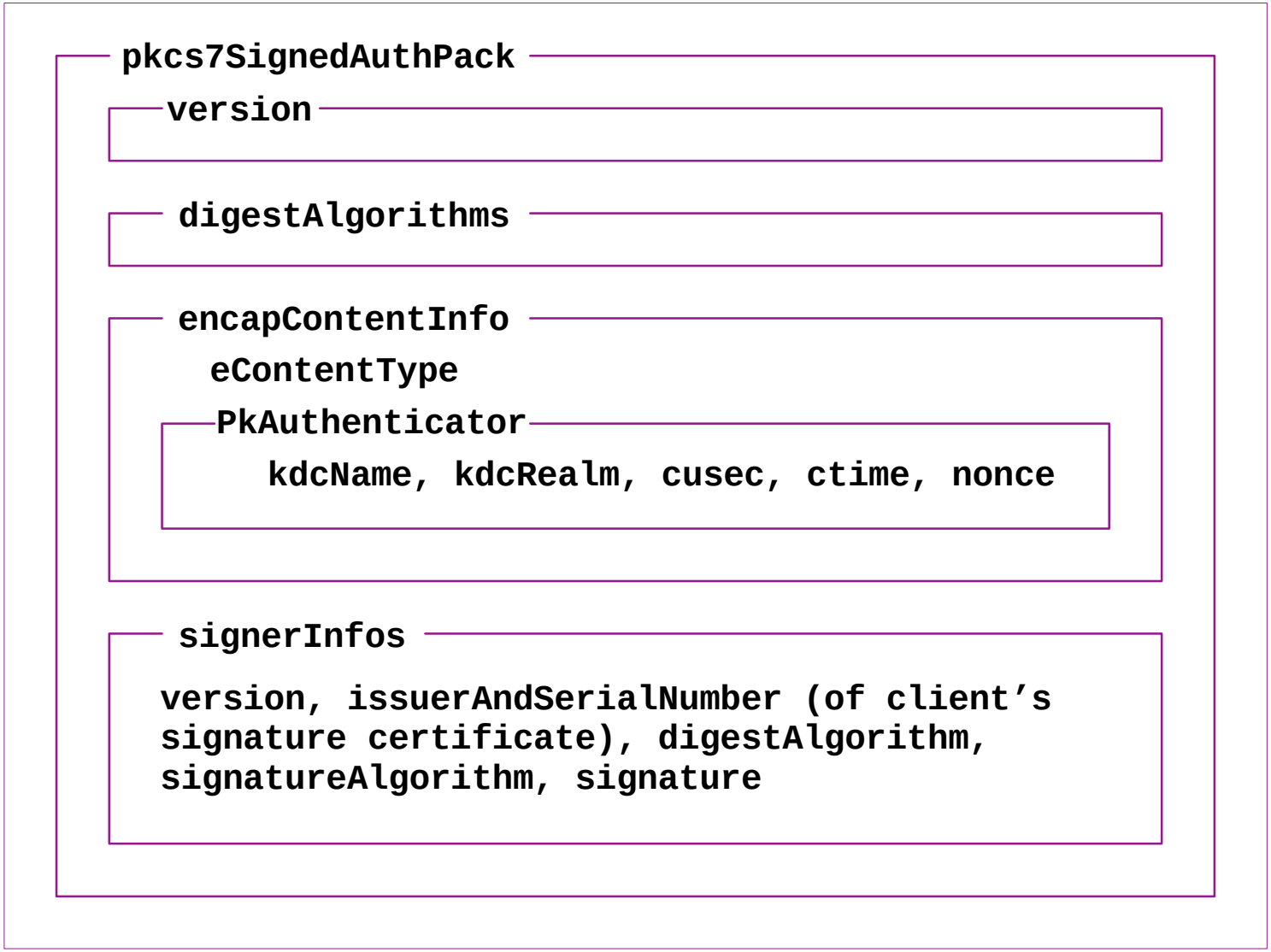
Application Using Cryptographic Services and Persistent Storage Services of a Class 2, PKCS#11 device



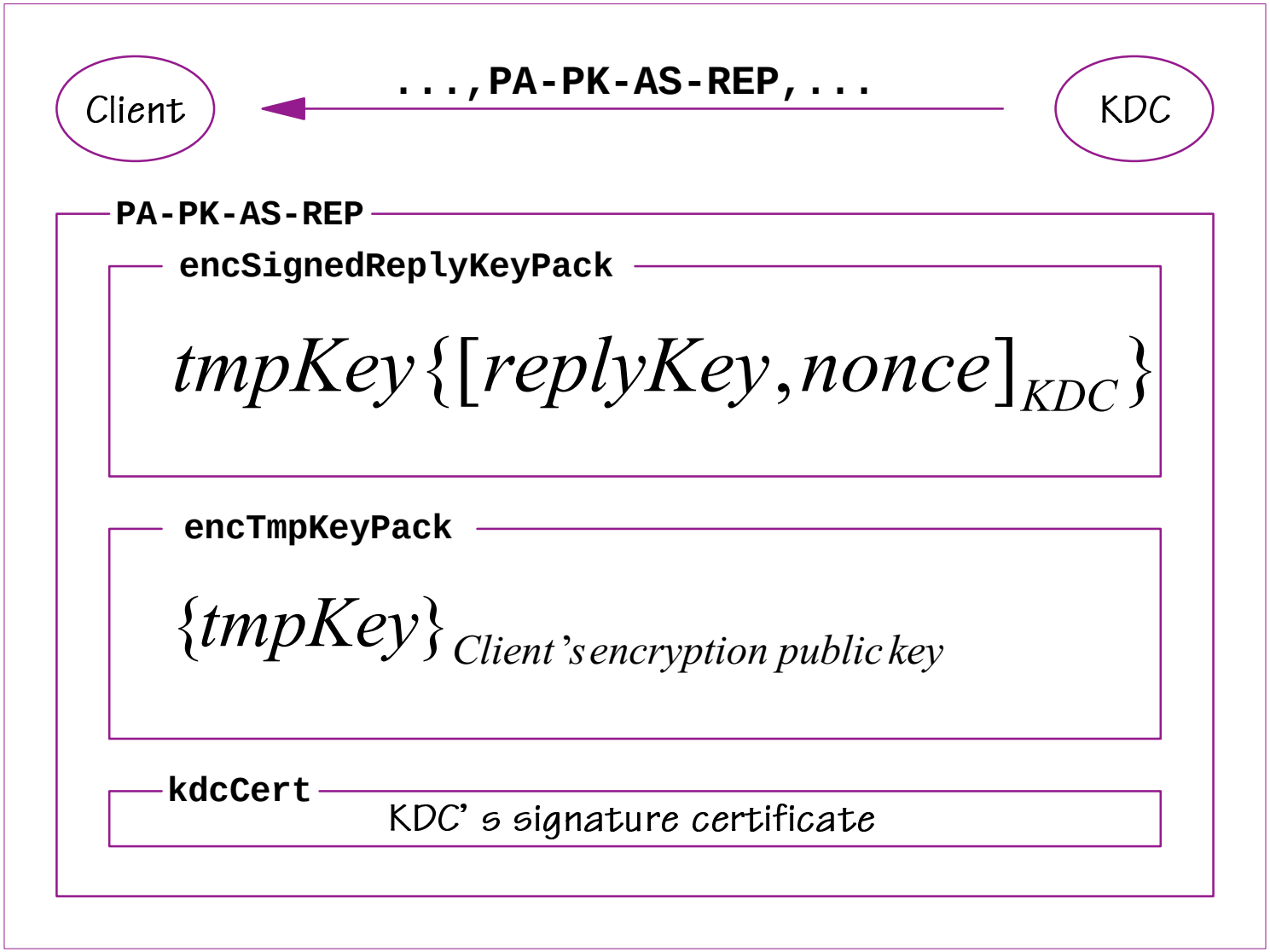
Client-to-KDC Message Overview



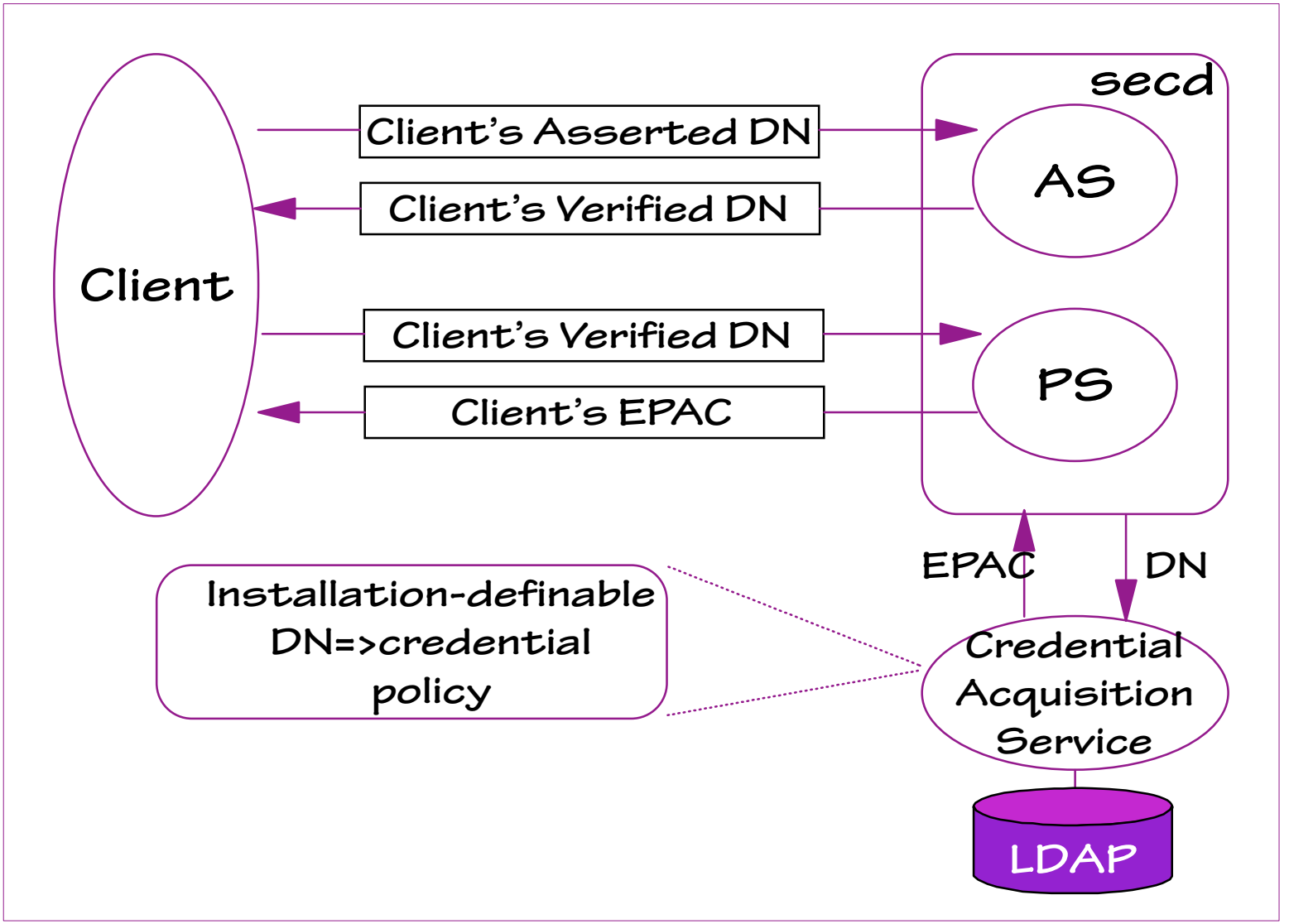
Details of CMS SignedData Object



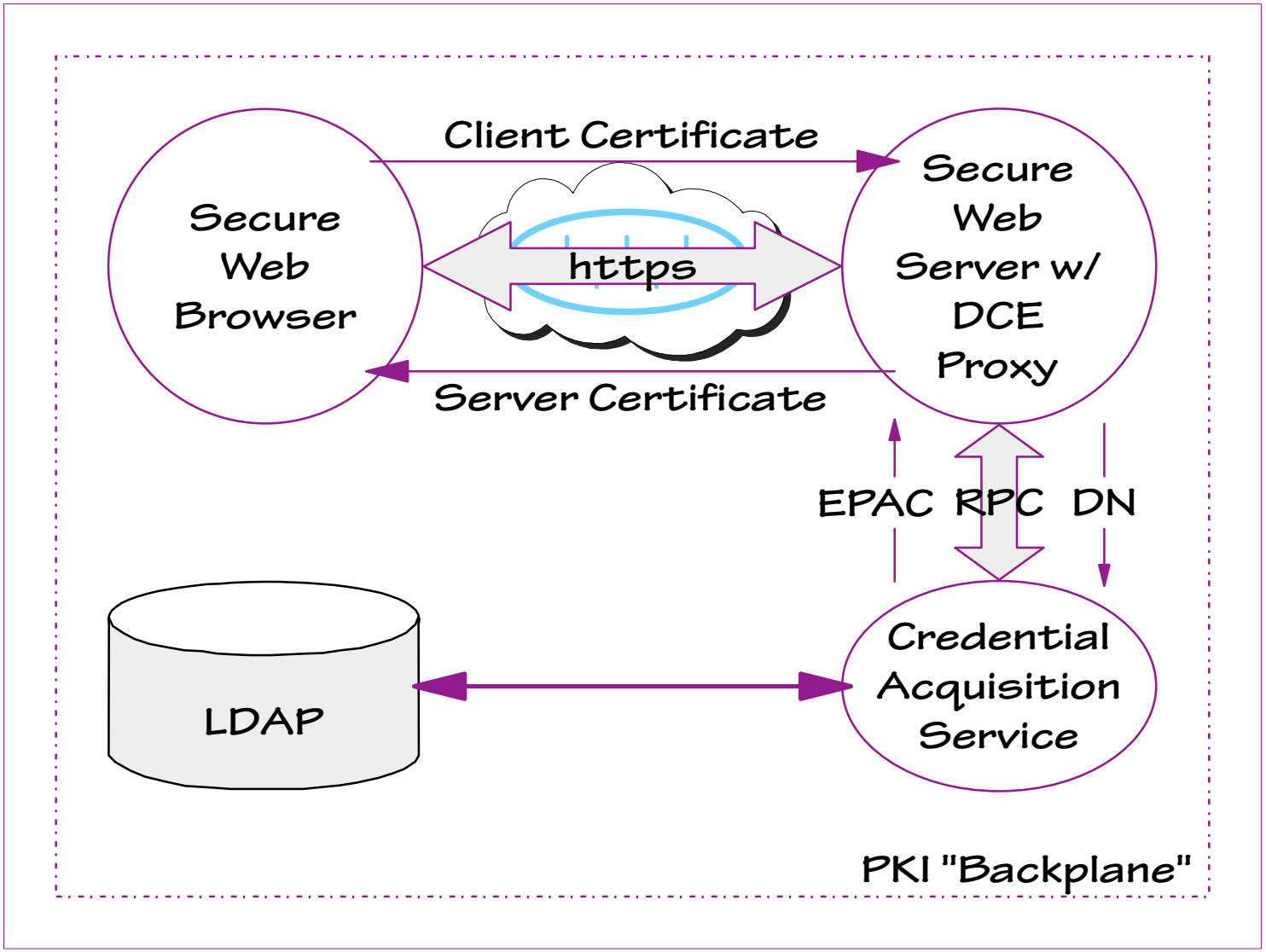
KDC-to-Client Response Overview



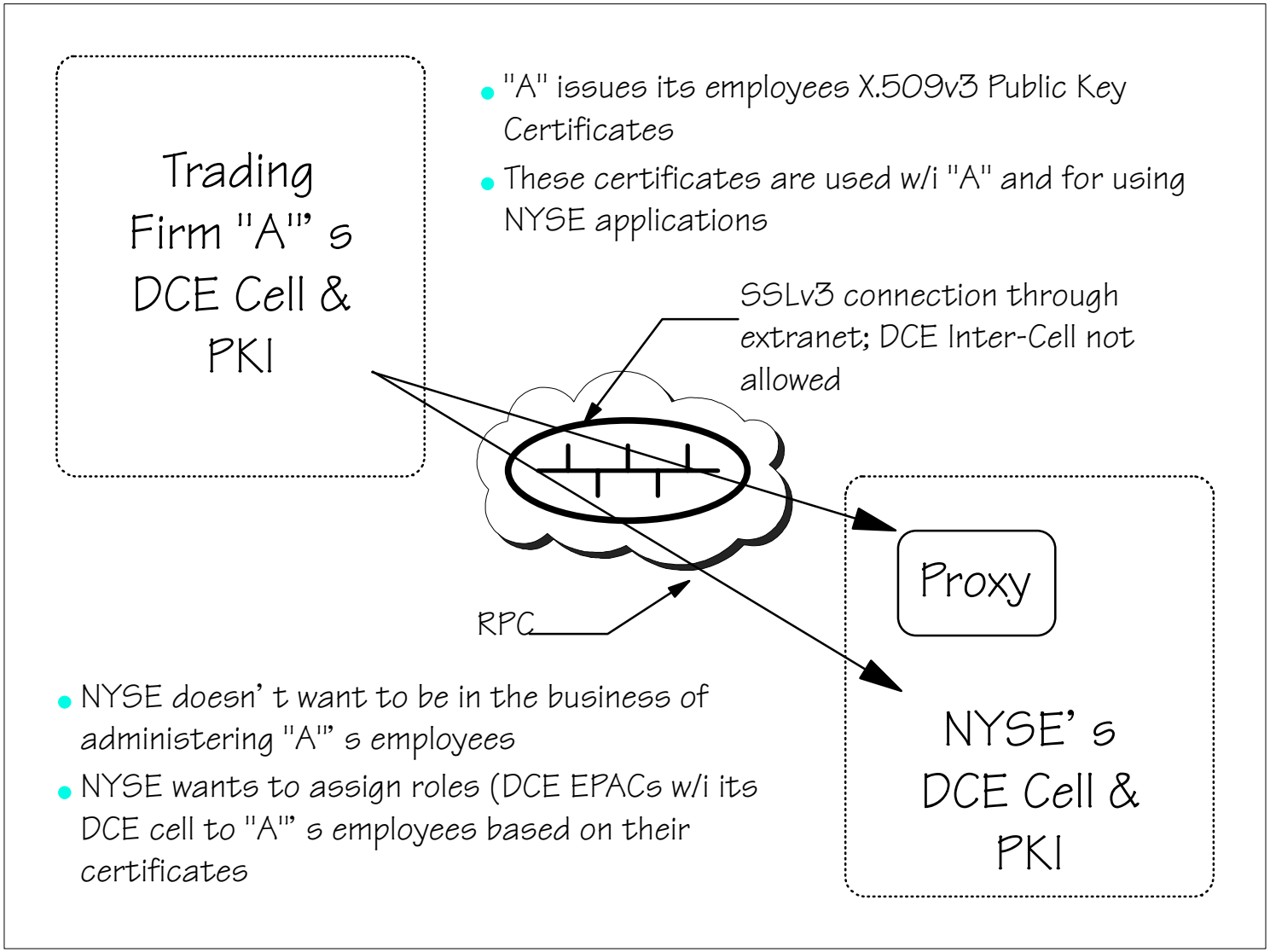
Credential Acquisition



Internet & DCE



SIMC/NYSE Scenario



The End-Goal

- Public Key Certificates for authentication
- DCE EPACs for authorization
- Over time eliminate the DCE Rgy as the holder of user information
  - Move to LDAP-accessed directories
- This "vision" ties in well with customer input
- It integrates with other "certificate-aware" applications
- It can better address the Internet space

Summary

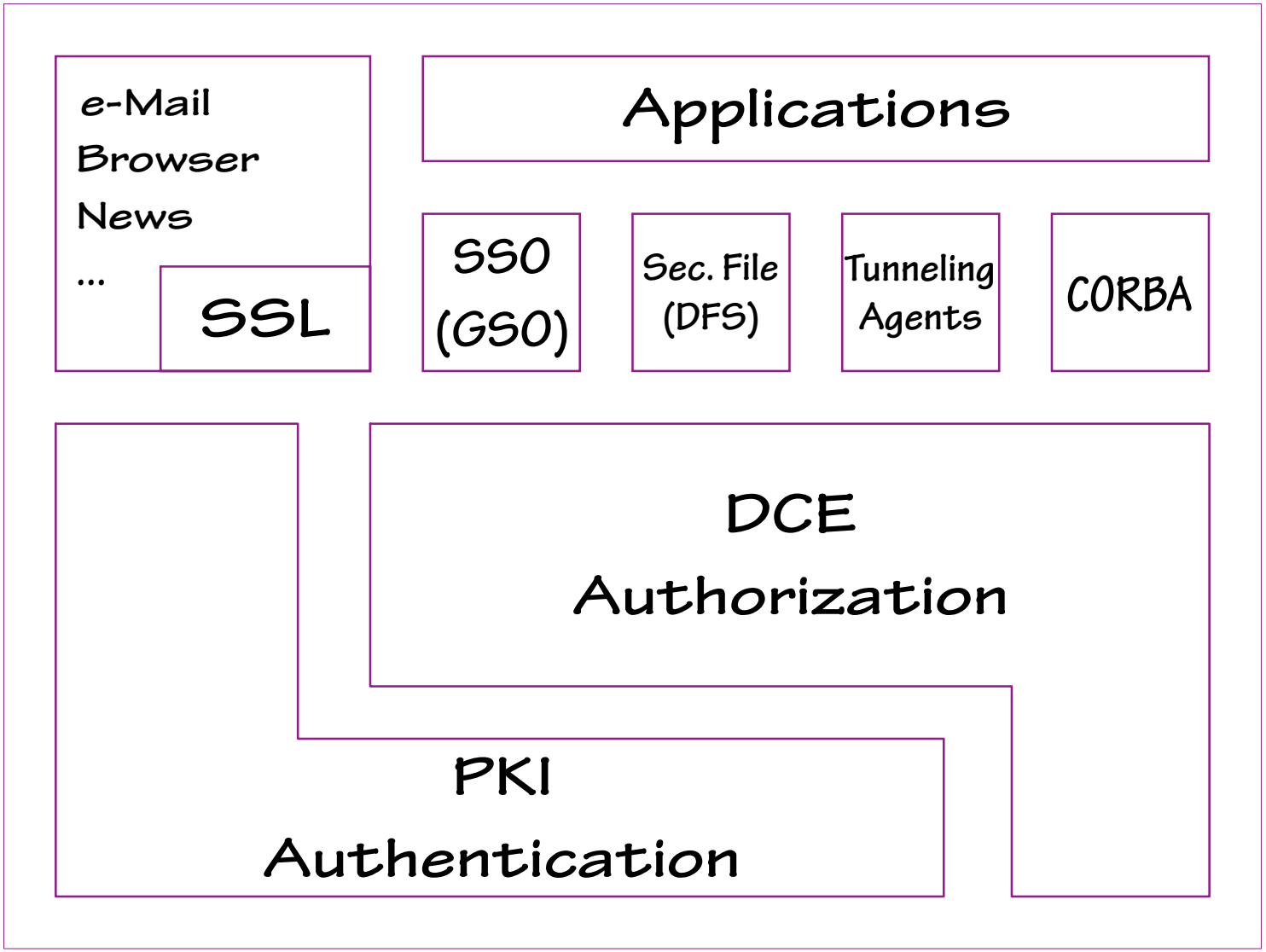
- RFC 68.4 is built on **open standards**
  - CDSA
  - CMS
  - Kerberos PK-INIT
- Work is correctly allocated
  - DCE is not a PKI, it's a consumer of PKIs
  - Potential for leveraging DCE as authorization system for PKIs
- This has truly been a collaborative effort
- TOG members' feedback sought

DASCOM & IBM Demo

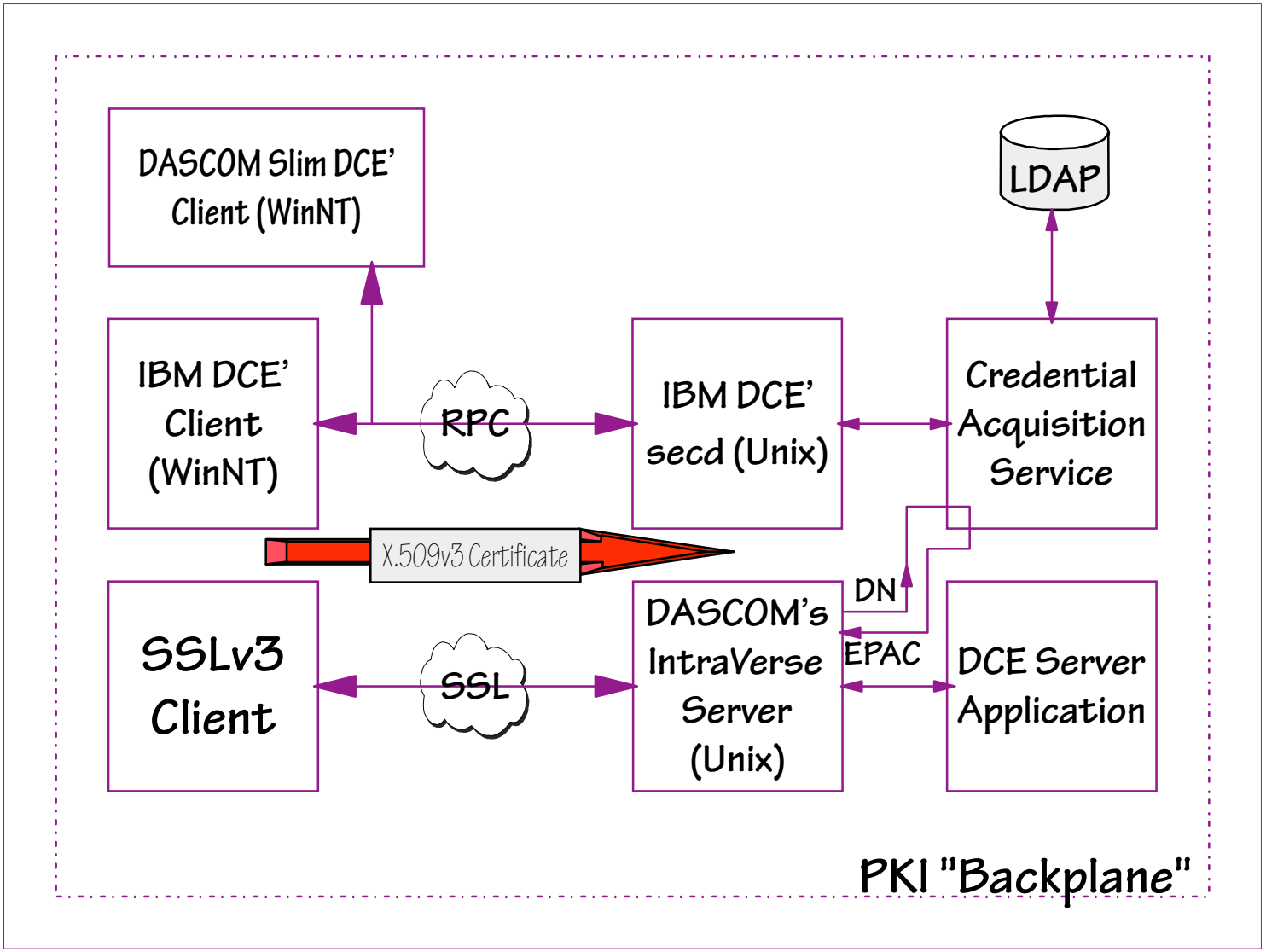
Kudos to the Development Team

- Peter Calvert, DASCOM
- Henry DeAngelis, IBM
- Sherif Ebady, IBM
- Ut Le, IBM
- David Reynolds, DASCOM

Enterprise Desktop Example/Solution
Digital Signature-Based Authentication



"Internetized" DCE



Users

- User definitions converge over time to LDAP
- Common authentication mechanism (X.509v3 public key certificates + digital signatures)
- Credential Acquisition Service provides flexible DN<=>EPAC mapping, *e.g.*,
  - Verisign Class 1 cert.: role=MinTrust
  - Cert. from trading partner: role=TrPrtnr
  - Cert. from enterprise's CA: role=RegEmpl
- DCE auditability maintained with DN as principal name