IEEE Std 1363-2000 and IEEE Std 1363a-2004

Ashley Butterworth
Apple Inc.

The Titles

- IEEE Std 1363-2000
  - IEEE Standard Specifications for Public-Key Cryptography
- IEED Std 1363a-2004
  - IEEE Standard Specifications for Public-Key Cryptography— Amendment 1: Additional Techniques

IEEE Std 1363-2000

- Scope (1363-2000 Clause 1.1)
  - This standard covers specifications for common public-key cryptographic techniques, including mathematical primitives for secret value (key) derivation, public-key encryption and digital signatures, and cryptographic schemes based on those primitives. Specifications of related cryptographic parameters, public keys, and private keys are also discussed. Classes of computers and communication systems are not restricted.

IEEE Std 1363a-20004

- Scope (1363a-2004 Clause 1.1)
  - Specifications of common public-key cryptographic techniques supplemental to those considered in IEEE Std 1363TM-2000, including mathematical primitives for secret value (key) derivation, public-key encryption, digital signatures, and identification, and cryptographic schemes based on those primitives, are provided. Specifications of related cryptographic parameters, public keys and private keys, are also provided. Class of computer and communications systems is not restricted.

General Model

- Primitives
  - Basic mathematical operations which are building blocks of schemes
- Schemes
  - A collection of operations combining primitives to provide a complexity-theoretic security
- Protocols
  - Sequence of operations combining schemes across multiple parties to achieve a security application.

Mathematical Conventions

- Notation
- Bit strings and Octet Strings
- Finite Fields
- Elliptic Curves
- Data Type Conversions

Discrete Logarithm Primitives

- Cryptography based on the Discrete Logarithm Problem
  - http://en.wikipedia.org/wiki/Discrete_logarithm
- Key and data definitions
- Primitives for converting from DL public + private keys to shared secrets
- Primitives for signing and verifying messages with DL private and public keys

Elliptic Curve Primitives

- Cryptography based on elliptic curve discrete logarithm problem
  - DL problem over an elliptic curve
- Key and data definitions
  - Primitives for converting from ECDL public + private keys to shared secrets
  - Primitives for signing and verifying messages with ECDL private and public keys

Integer Factorization Primitives

- Cryptography based on Integer Factorization Problem
  - http://en.wikipedia.org/wiki/Integer_factorization
  - RSA is a type of IF
- Key and data definitions
- Primitives for
  - Encryption and Decryption
  - Signing and Verification

Schemes

- Key agreement
  - Creating a shared secret from public and private keys
- Signature
  - Verifying that the message is from the signer and hasn’t been tampered with
- Encryption
  - Creating a cipher text from plain text and converting it back

Key Agreement Schemes

- Creates a shared secret from the public and private keys of two parties
  - Party A generates the secret with his private key and party B's public key
  - Party B generates the secret with his private key and party A's public key
- Other info may be combined in the secret generation

Signature Schemes

- Signer generates a signature for the message based on the signer's private key
- Verifier verifies the signature with the signers public key
- IEEE 1363a has five
  - DL/EC signature schemes (DL/ECSSA, DL/ECSSR, DL/ECSSR-PV)
  - IF signature schemes (IFSSA, IFSSR)

Encryption Schemes

- Encrypting and decrypting messages
- IEEE 1363a defines three
  - IF encryption scheme (IFES, IFES-EPOC)
  - DL/EC encryption scheme (DL/ECIES)

Message Encoding Methods

- Methods for Signing with appendix or message recovery
  - Creates a representation of the message (hash) which can be used in the signing and verification math and defines signing & verification processes
    - Method for DL/ECSSA
    - Method for IFSSA
- Methods for Encryption
  - Defines how to encode and decode message for IFES

Auxiliary Functions

- Hash functions
  - Standard ones and where they are defined
- Mask generation functions
- Symmetric encryption schemes
- Message authentication codes

How does this apply to 1722a

- Signature Schemes
  - IF based signature scheme (IFSSA) for verifying packets are from the sender
    - Keys are managed by IEEE P1722.1 or in a vendor unique way
- Key Agreement Schemes
  - Generate a shared secret for AES or other symmetric key encryption system
- Encryption Schemes
  - IFES is too heavyweight for small devices
  - Look at other schemes (AES, etc)

How does this apply to 1722.1

- 1722.1 provides the key management
  - Gets public key's from Entity and uses an IFSSA based chain of trust on the keys back to a root key
  - Adds keys to and removes keys from the Entity
    - Other public and private keys
    - Symmetric (AES) keys
- 1722.1 relies on the 1722a use of signing and/or encryption to prove that the PDU is from the Entity or Controller and to provide protection of authentication and key transport

How is 1722.1 using 1363a-2004

- Full details in 7.6 of 1722.1 D20
  - Also see Authentication and Security presentation tomorrow
- 1722.1 uses the IFSSA to establish chain of trust on keys and as verification of Entity model
  - Uses
    - IFSP-RSA1 for signing
    - IFVP-RSA1 for verification
    - EMSA2 with a SHA256 hash for message encoding