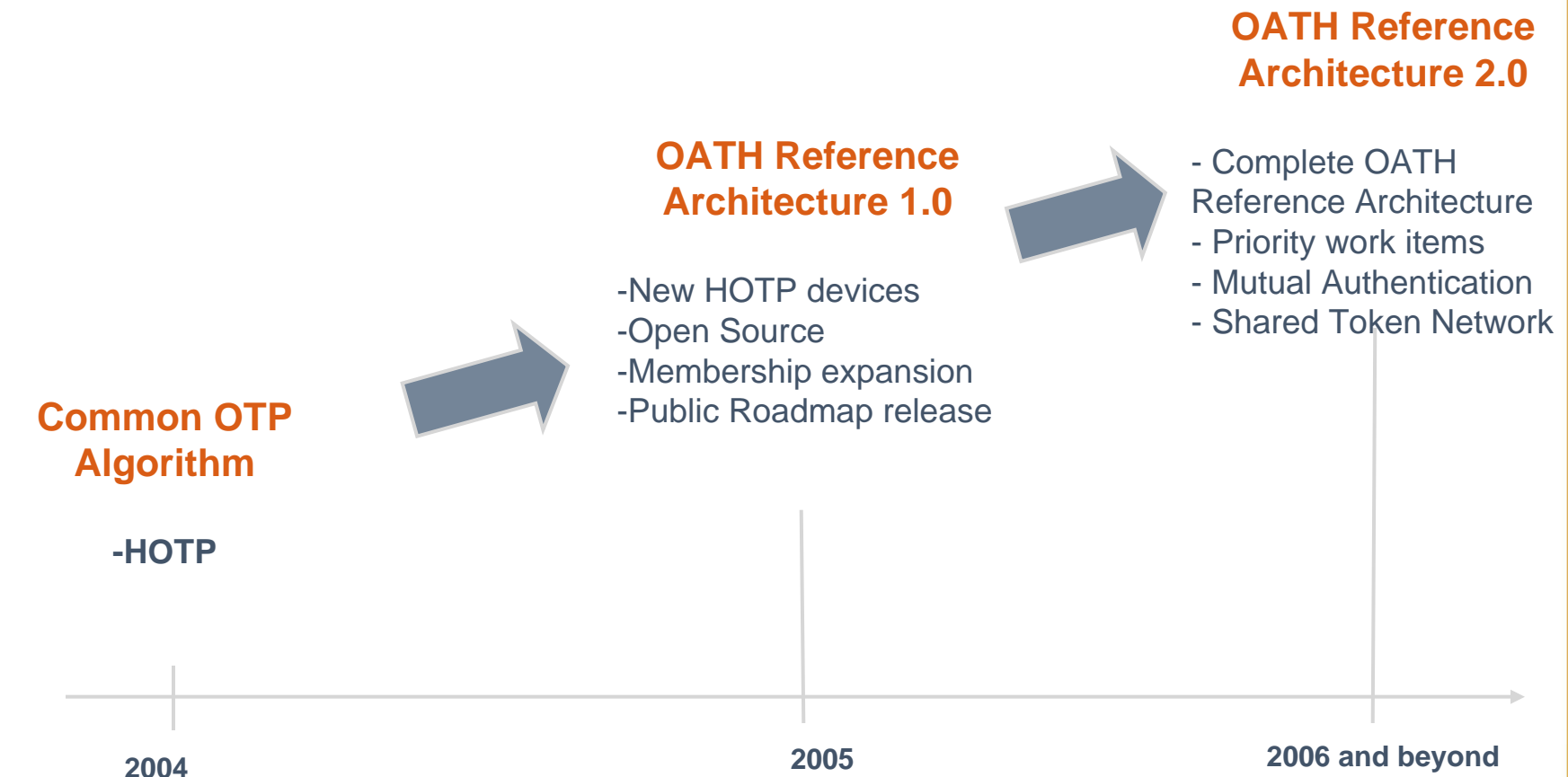




OATH Roadmap

November 22nd, 2005

OATH Progress



A humble beginning!

Momentum is building...

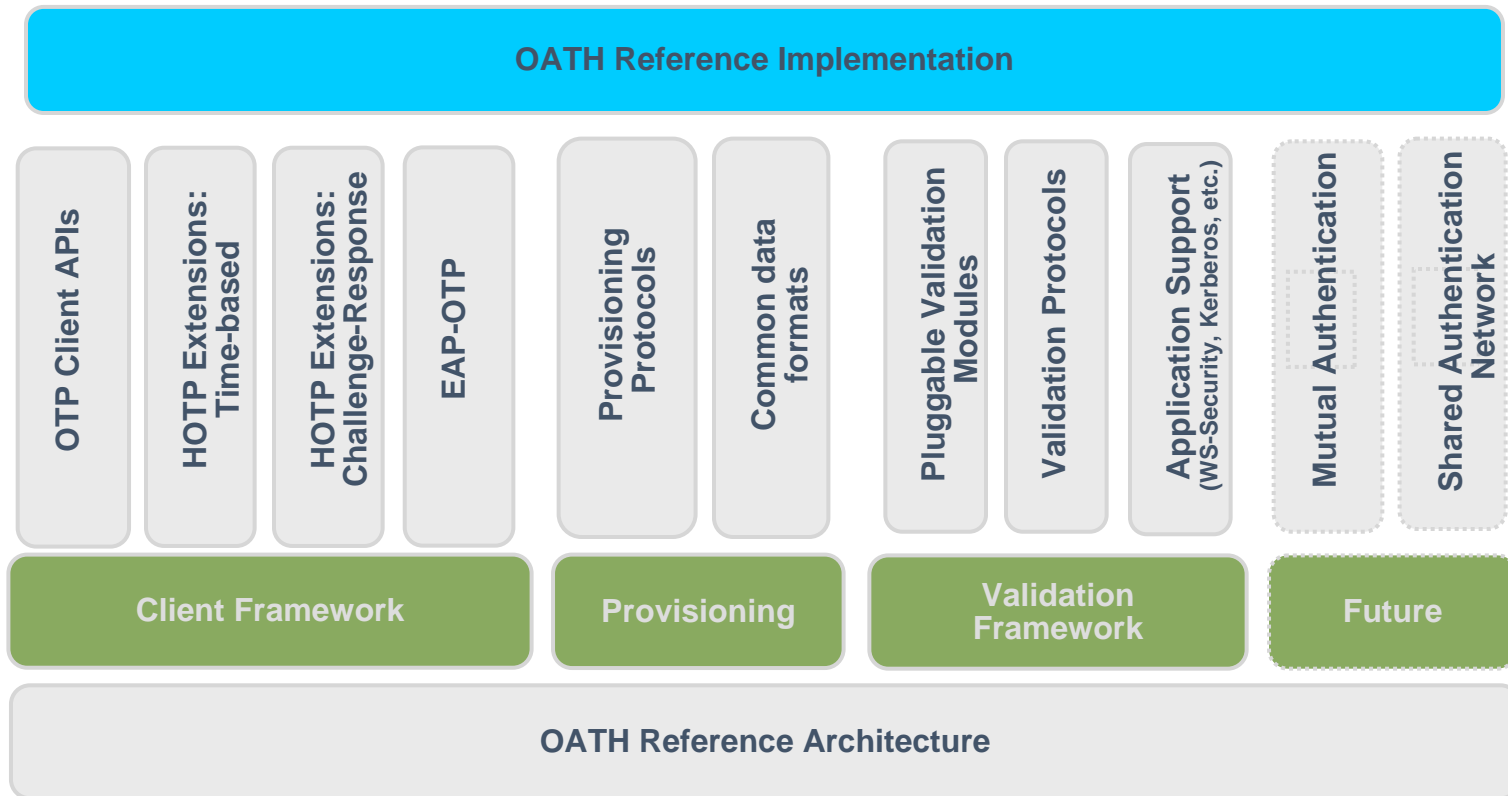
OATH Objectives

- **4 Guiding Principles**
 - Device Innovation and Embedding
 - Interoperable Modules
 - Native platform support
 - Open and royalty-free specifications
- **Benefits**
 - Drives innovation and vendor adoption
 - Promotes interoperability and open architectures
 - Lower costs for customers, software and hardware vendors

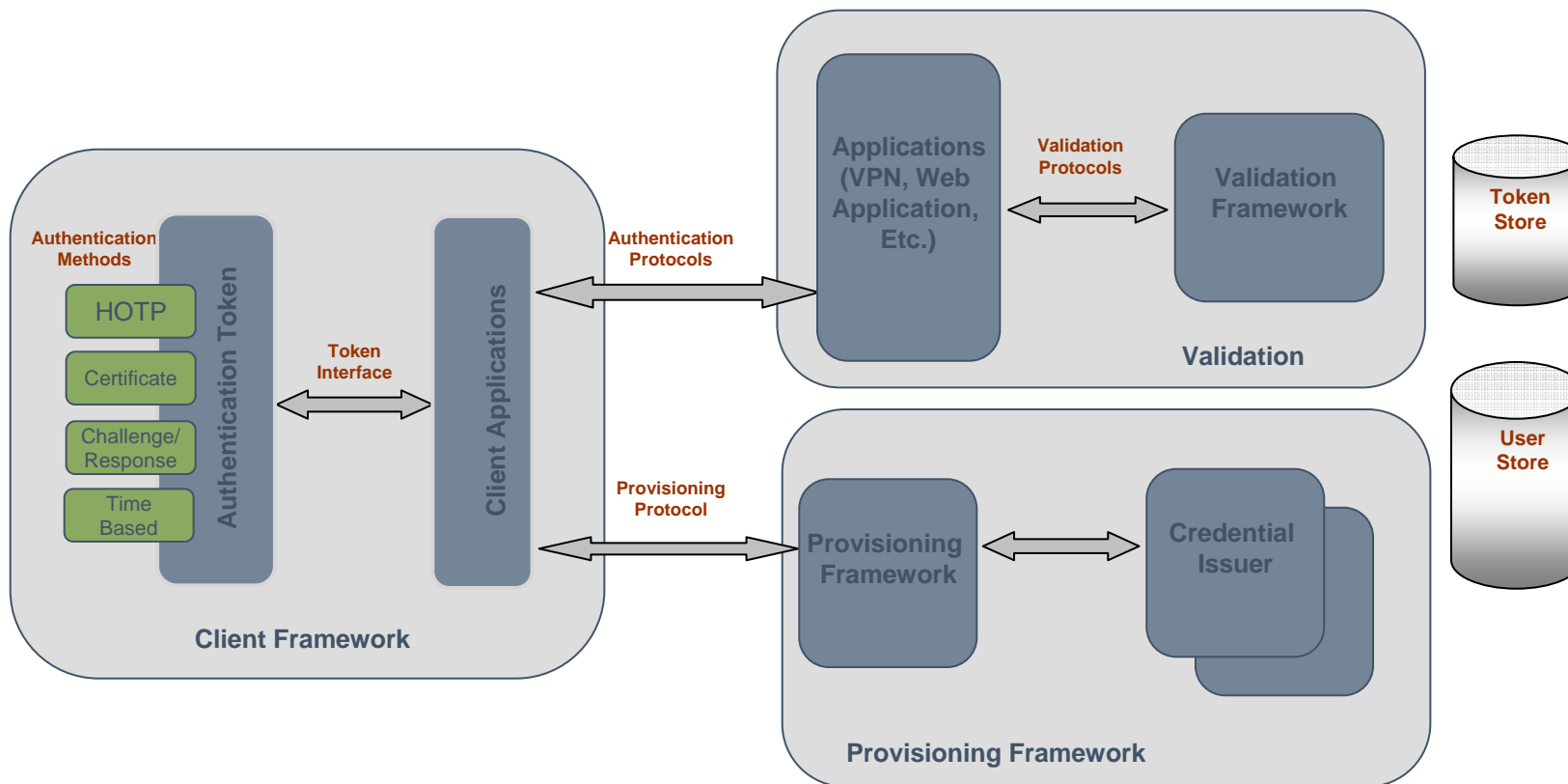
OATH Advantages

- **Established leadership**
(working on the problem space for two years)
- **Large base of technology and industry leaders**
- **Neutral stance enables coordination with multiple standard bodies**
- **Open and royalty-free specification**

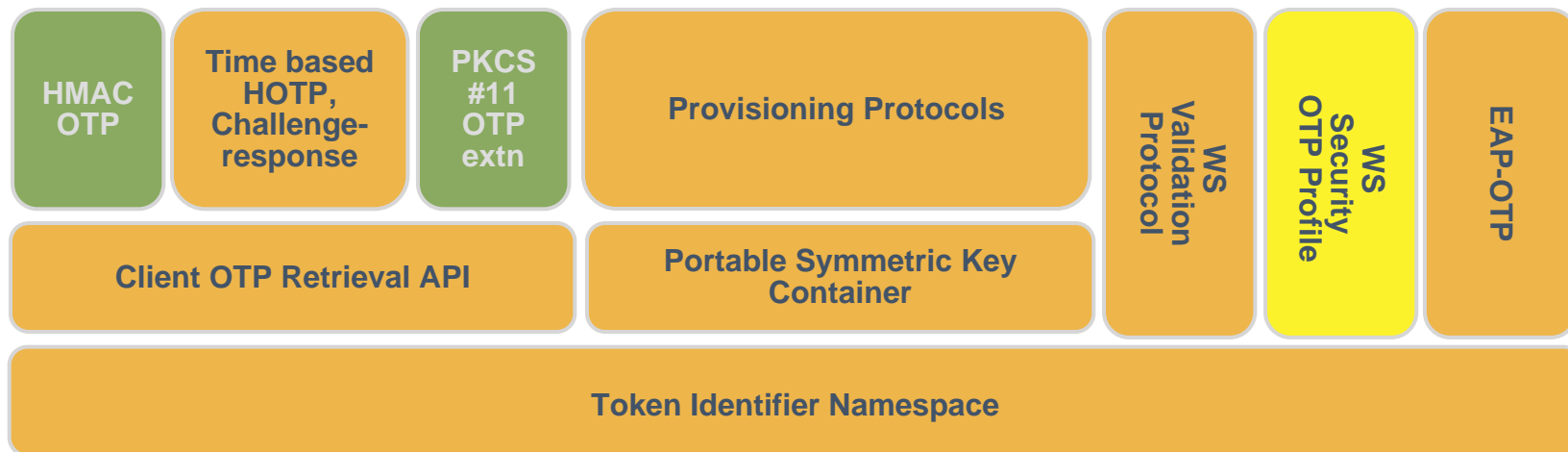
OATH Deliverables



OATH Architecture View



2006 Focus Areas



 Completed  2006 priority item  In progress

2006 Timeline

- **H106**
 - HOTP Extensions (Time, Challenge/Response)
 - Token ID Namespace
 - Web Services OTP Validation Protocol
 - Portable Symmetric Key Container
- **H206**
 - WS-Security Token for OTP
 - Symmetric Key Provisioning Protocols
 - OTP Retrieval Client API
 - EAP method for OTP

HOTP Extensions

- **Description**

- Challenge/Response
- Digital Signatures
- Time-based OTP

- **Benefits**

- Drive innovation for other devices
 - We have already seen excellent adoption rates for HOTP!
- Offer more choice to customers
 - One size does not fit all

Token ID namespace

- **Description**

- Creates an industry standard naming convention that allows unique naming of any OATH compliant token across all vendors.

- **Benefits**

- Interoperability
 - enables mix and match scenario where you can use tokens from one vendor and software and middleware from another vendor
 - enables software vendors to implement support for just one token ID convention rather than supporting a different one per vendor.
- Enable applications such as discovery services in the future.

Web Services Validation Protocol

- **Description**

- A web services means to validate OTP and other symmetric key based credentials.

- **Benefit**

- Extends support for OTP beyond the traditional RADIUS protocol
- Support for Service Oriented Architectures (SOA).

Portable Symmetric Key Container

- **Description**

- Creates a standard and portable format to communicate symmetric key credentials between different modules.

- **Benefit**

- Interoperability across vendors
 - Enables mix-and-match scenarios
- Easy migration and maintenance

WS Security OTP profile

- **Description**

- Create a new WS-Security token type for one-time passwords.

- **Benefit**

- Enables use of various OTP-based authentication methods within the WS-Security framework.

Symmetric Key Provisioning Protocols

- **Description**

- A client-server protocol to enable a client device to download and install authentication credentials from a provisioning server in a secure and efficient manner.

- **Benefit**

- Embedding and device innovation
 - Enable a variety of embedded form-factors such as phones, USB tokens, software tokens, etc.

OTP Client API

- **Description**

- Enable the retrieval of OTP values from a variety of tokens (software and connected hardware)

- **Benefit**

- End-user Usability
- Simple interface for applications to retrieve OTP credentials.
 - Easy to implement
 - Multi-platform availability
 - One API for a variety of hard, soft and on-board tokens

EAP Method for OTP

- **Description**

- An extension of EAP protocol for authenticating to wireless networks

- **Benefit**

- Helps secure enterprise and public WiFi networks
 - Enabling various OTP based authentication methods within the EAP framework.

2006 and beyond

- **Complete Phase 2 work items**
 - *Validation Handler Interface*
 - *LDAP Schema Extension*
 - *Dynamic discovery of token validation node*
 - *Client OTP Provisioning/Mgmt API*
- **Mutual Authentication**
- **Shared Authentication Network**



Thank You!