# Internet Engineering Task Force
# Provisioning of Symmetric Keys Working Group

Hannes Tschofenig

# Agenda

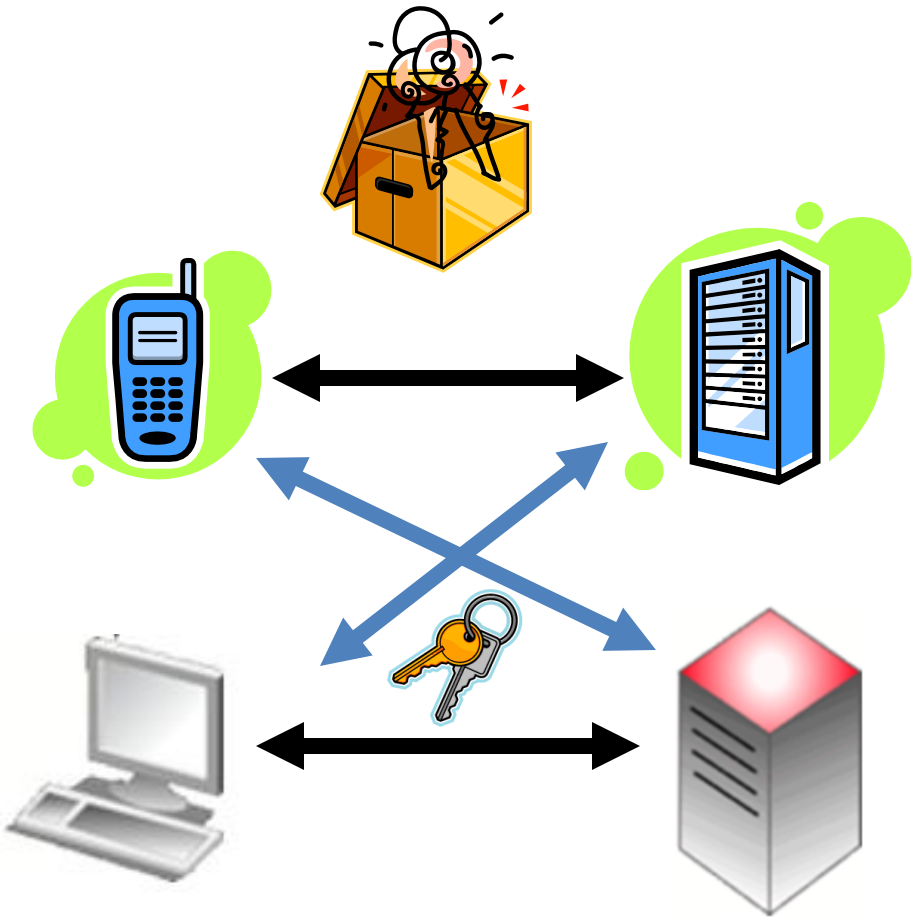
- Brief History of IETF KEYPROV Working Group
- OTP Example
- PSKC
- DSKPP

# IETF KEYPROV Working Group: Why?

- Starting point for KEYPROV working group formation early 2007:
  - Vendor-specific solutions for provisioning one-time passwords (and meta-data) but no standardized solution available.
- Provisioning scenarios included
  - over the wire
  - over the air
  - or offline (bulk)
- No standardized container for keys and meta-data available either.

# IETF KEYPROV Working Group: Why? (Cont.)

- No interoperability
  - between client and servers for provisioning symmetric keys.
  - between servers from different vendors.



# IETF KEYPROV Working Group

- Description

  Current developments in deployment of Shared Symmetric Key (SSK) tokens have highlighted the need for a standard protocol for provisioning symmetric keys.

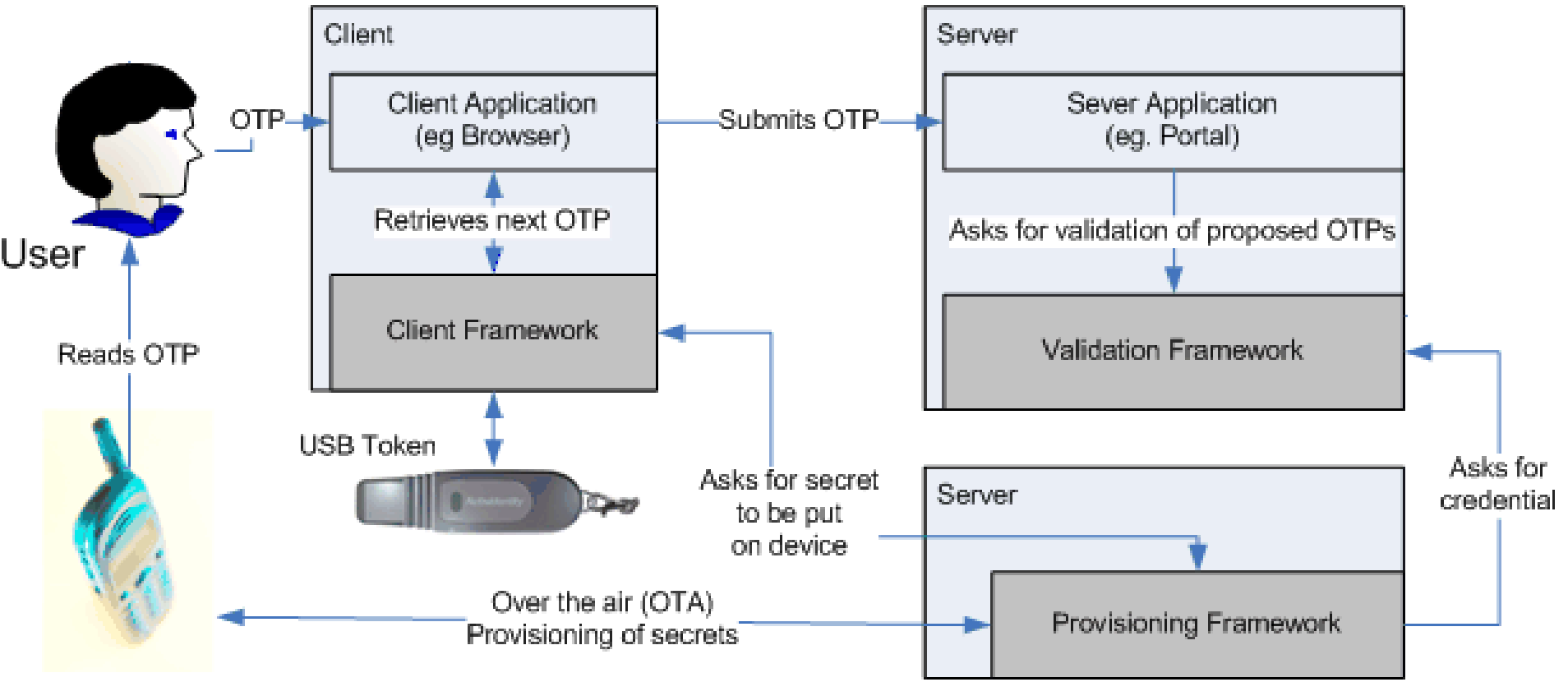
  The need for provisioning protocols in PKI architectures has been recognized for some time. Although the existence and architecture of these protocols provides a feasibility proof for the KEYPROV work assumptions built into these protocols mean that it is not possible to apply them to symmetric key architectures without substantial modification.

  In particular the ability to provision symmetric keys and associated attributes dynamically to already issued devices such as cell phones and USB drives is highly desirable.

# IETF KEYPROV Working Group: Scope and Deliverables

- Scope
  - The scope of the working group shall be to define protocols and data formats necessary for provisioning of symmetric cryptographic keys and associated attributes.
  - The group shall consider use cases related to use of Shared Symmetric Key Tokens. Other use cases may be considered for the purpose of avoiding unnecessary restrictions in the design and ensure the potential for future extensibility.
- Deliverables:
  - Dynamic Symmetric Key Provisioning Protocol
    - http://tools.ietf.org/wg/keyprov/draft-ietf-keyprov-dskpp/
  - Portable Symmetric Key Container (XML)
    - http://tools.ietf.org/wg/keyprov/draft-ietf-keyprov-pskc/
  - Symmetric Key Package Content Type (ASN.1)
    - http://tools.ietf.org/wg/keyprov/draft-ietf-keyprov-symmetrickeyformat/

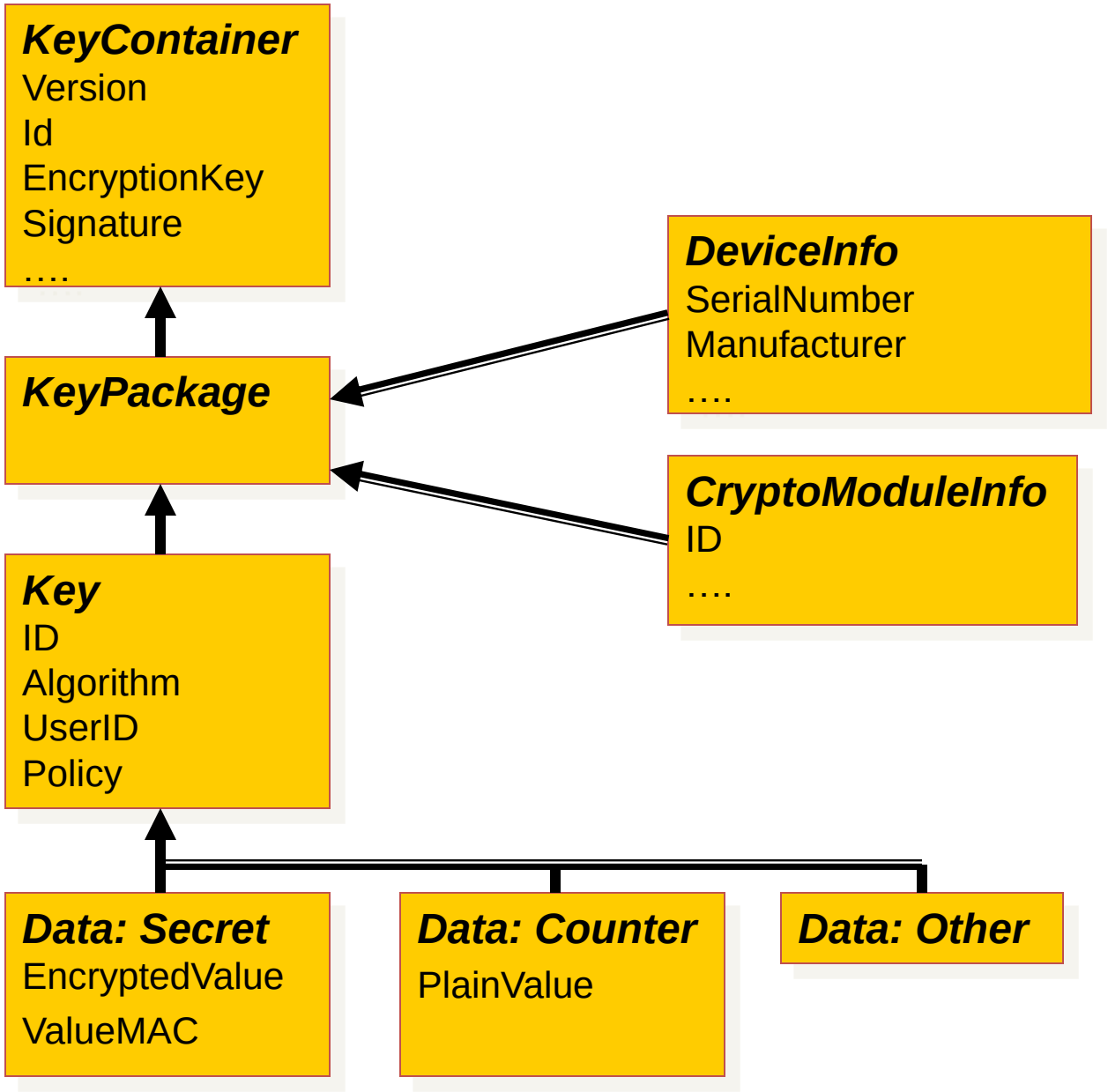
# OTP Example


Client
Client Application
(eg Browser)
Retrieves next OTP
Client Framework
OTP
User
Reads OTP
USB Token
Submits OTP
Server
Sever Application
(eg. Portal)
Asks for validation of proposed OTPs
Validation Framework
Asks for secret
to be put
on device
Server
Provisioning Framework
Asks for
credential
Over the air (OTA)
Provisioning of secrets

# PSKC: Overview

- Portable Symmetric Key Container (PSKC) is a standardized XML-based document for transporting symmetric keys and key related meta data.
- Specifies the information elements that may be required when the symmetric key is utilized for specific purposes, such as the initial counter in the HOTP algorithm.
- Requests the creation of a IANA maintained registry for PSKC algorithm profiles:
  - Such a profile contains a common name, pointer to a stable reference, URN for reference to the profile, information about PSKC XML elements and attributes being used, and examples.
  - PSKC spec defines two PSKC algorithm profiles: HOTP and KEYPROV-PIN
  - Further algorithm profiles are described in draft-hoyer-keyprov-pskc-algorithm-profiles.
- An symmetric key container using an ASN.1 based encoding is available with draft-ietf-keyprov-symmetrickeyformat.

# PSKC: Data Model



# PSKC: Basic Example

```
<?xml version="1.0" encoding="UTF-8"?>
 <KeyContainer Version="1.0"
    Id="exampleID1"
    xmlns="urn:ietf:params:xml:ns:keyprov:pskc">
    <KeyPackage>
       <Key Id="12345678"
          Algorithm="urn:ietf:params:xml:ns:keyprov:pskc#hotp">
          <Issuer>Issuer-A</Issuer>
          <Data>
             <Secret>
                <PlainValue>MTIzNA==
                </PlainValue>
             </Secret>
          </Data>
       </Key>
    </KeyPackage>
 </KeyContainer>
```

# PSKC: Key Protection Methods

- Various options:
  - Protection by underlying transport.
  - Pre-shared symmetric keys
    - For those cases where the encryption algorithm does not provide integrity protection an additional MAC key and MAC algorithm
  - Password based encryption
    - Key derived from password based on PKCS#5.
    - XML Encryption 1.1 is used.
  - Asymmetric  keys
    - Information about the used certificate must be included in the Key Container
    - Encryption of secret with the help of XML Encryption.
- Digital signature can be applied to the entire <KeyContainer>

# PSKC: Misc Features

- Bulk provisioning capabilities
  - Multiple Key Packages within a single Key Container.
- Ability to carry a key policy
  - Start & Expire Date
  - Restriction on the number of key usages
  - PIN protection policy
  - Registry for key usage, such as “OTP”, “CR”, “Encrypt” (based on NIST SP800-57 )

# Example: HOTP Algorithm Profile

Common Name: HOTP

Class: OTP

URN: urn:ietf:params:xml:ns:keyprov:pskc#hotp

Algorithm Definition: http://www.ietf.org/rfc/rfc4226.txt

Identifier Definition: PSKC RFC

Profiling:

- The <KeyPackage> element MUST be present and the <ResponseFormat> element, which is a child element of the <AlgorithmParameters> element, MUST be used to indicate the OTP length and the value format.
- The <Counter> element MUST be provided as meta-data for the key.
- The following additional constraints apply:
  - The value of the <Secret> element MUST contain key material with a length of at least 16 octets (128 bits), if it is present.
  - The <ResponseFormat> element MUST have the 'Format‘ attribute set to "DECIMAL", and the 'Length' attribute MUST indicate a length value between 6 and 9 (inclusive).
  - The <PINPolicy> element MAY be present but the 'PINUsageMode' attribute cannot be set to "Algorithmic".

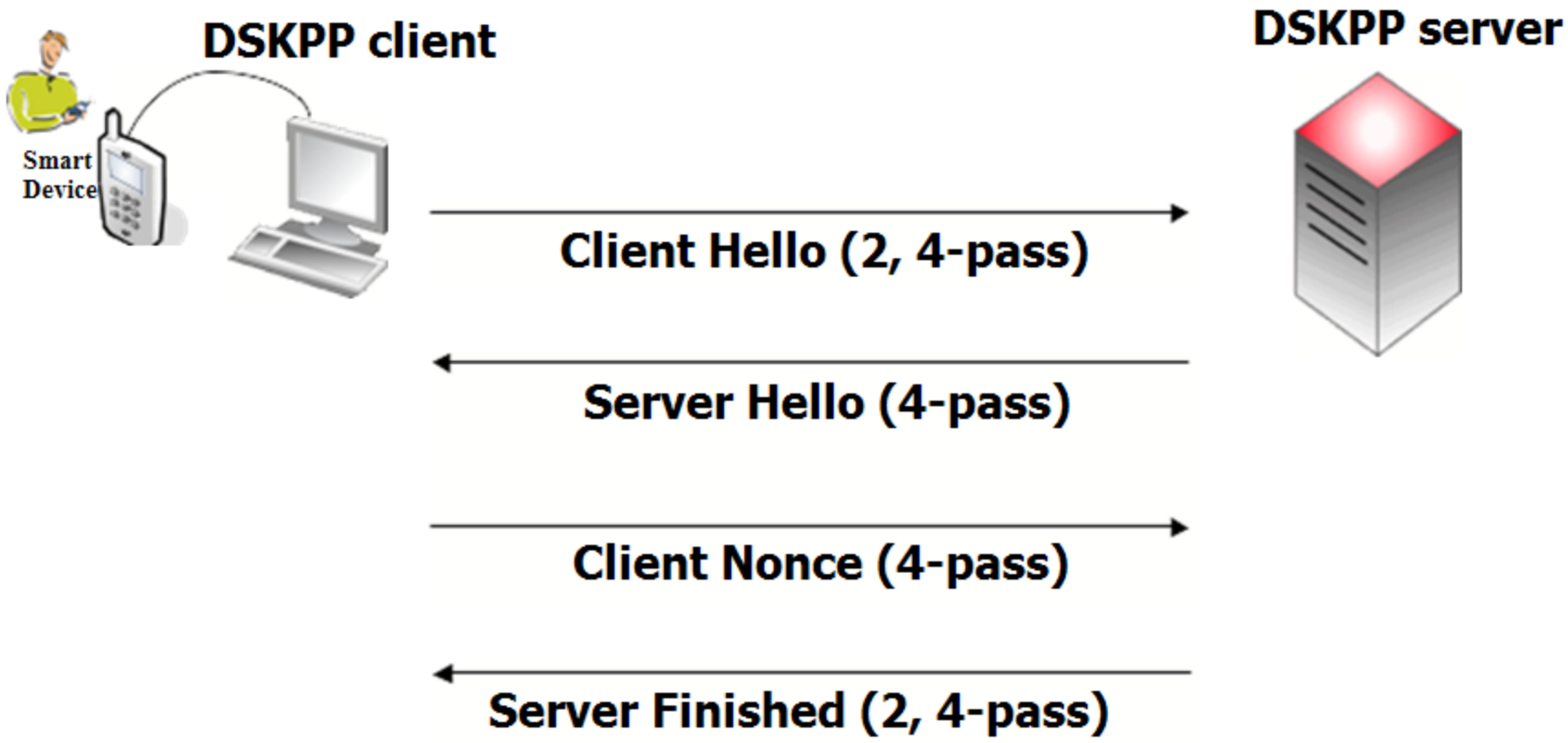
# DSKPP: Overview

- The Dynamic Symmetric Key Provisioning Protocol (DSKPP) is a client-server protocol for initialization (and configuration) of symmetric keys to cryptographic modules.
- Can be run
  - with or without private-key capabilities in the cryptographic modules, and
  - with or without an established public key infrastructure.

# DSKPP: Protocol Variants

- DSKPP variants support multiple usage scenarios:
  - Four-pass variant enables joint key generation by the provisioning server and cryptographic module; provisioned keys are not transferred over-the-wire or over-the-air.
  - Two-pass variant enables generation and transport of symmetric keys to a cryptographic module.
  - Two-pass variant also enables transport of pre-generated (e.g., legacy) keys to a cryptographic module.

# DSKPP: Two-Pass and Four-Pass



# DSKPP: Cryptographic Properties

- Key confirmation
  - In both variants via MAC on exchanged data
- Replay protection
  - In both variants through inclusion of client-provided data in MAC
- Server authentication
  - In both variants through MAC in ServerFinished message when replacing existing key
- Protection against MITM
  - In both variants through use of shared keys, client certificates, or server public key usage
- User authentication
  - Enabled in both variants using authentication code
- Device authentication
  - In both variants if based on shared secret key or if device sends a client certificate

# DSKPP: Transport

- Security Binding
  - Transport Layer Security is not required for key transport
  - TLS useful for confidentiality protection of the exchanged parameters.
- Defined HTTP transport binding
  - New MIME-type registered.
  - No SOAP binding standardized because not useful.

# Summary

- Three specifications developed within KEYPROV:
  - DSKPP – Online symmetric key provisioning protocol
  - PSKC – XML based symmetric key container format
  - ASN.1 based symmetric key container
- In late stages of the IETF document life cycle
- Two other documents being published (outside the KEYPROV WG) as AD-sponsored documents that are relevant for the work:
  - TOTP as a variant of the HMAC-Based One-Time Password (HOTP) (see draft-mraihi-totp-timebased)
  - OATH Challenge-Response Algorithms (OCRA) (see draft-mraihi-mutual-oath-hotp-variants)

# IETF Open Web Authentication (OAuth)


- OAuth is about delegated authentication
- Offers secure access to data for Web applications on the Internet
- "OAuth is shaping up as the cornerstone of identity management for cloud-based applications and services"

  http://www.eweek.com/c/a/Security/OAuth-Is-the-New-Hotness-In-Identity-Management-572745/
- IETF OAuth WG Charter: http://www.ietf.org/html.charters/oauth-charter.html