Using Token Based Authentication

Andrina Kelly - IronGate Server Management & Consulting
James Turner - CRYPTOCard

IronGate
SERVER MANAGEMENT & CONSULTING

Why should I be thinking about stronger authentication? Look what I've got already...

- Password Policies
- Educated Users
- VPN
- Physical Security

So did these people...









So did these people...



3.9 Million Card & PIN Combos stolen







So did these people...

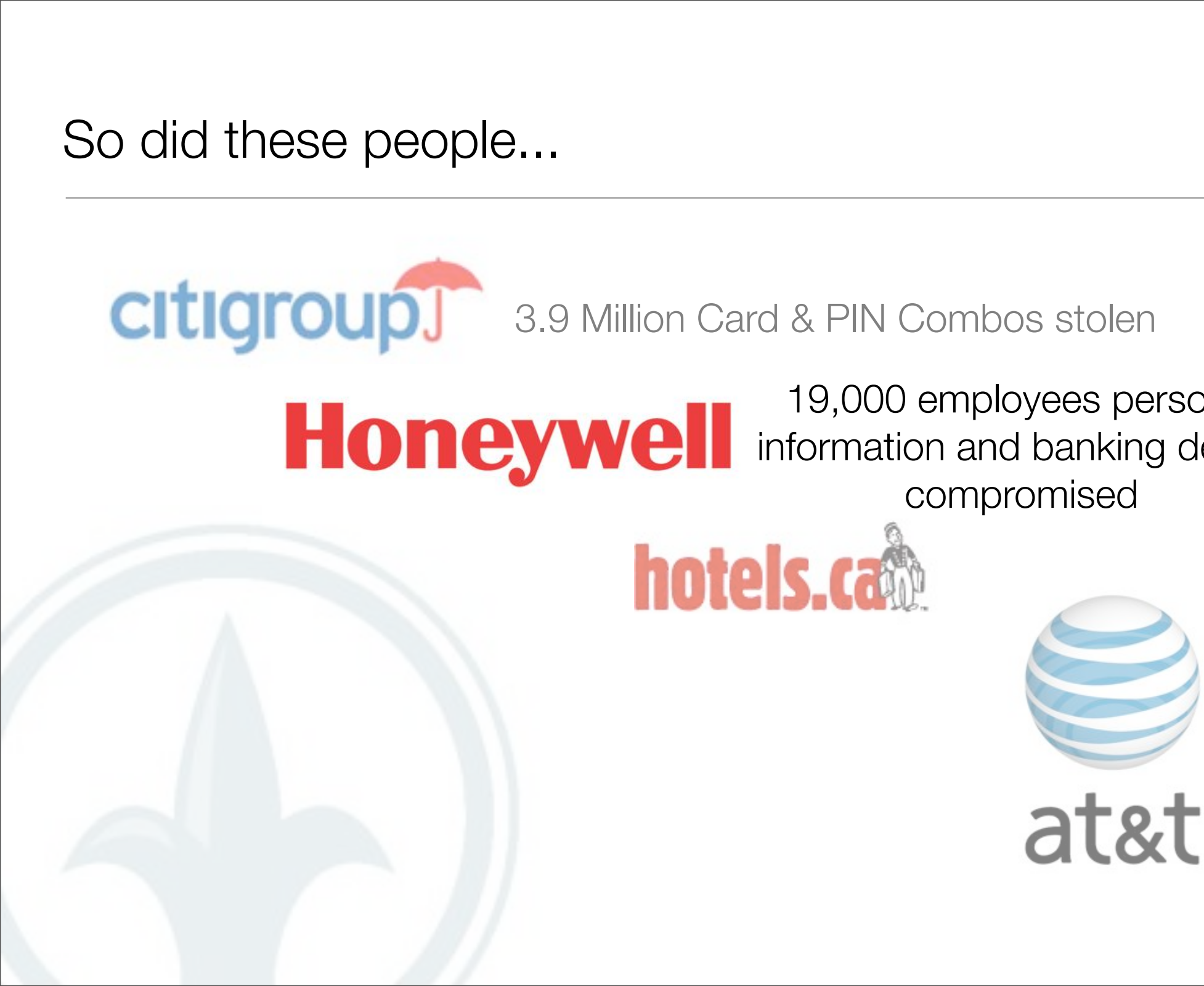
citigroup

3.9 Million Card & PIN Combos stolen

Honeywell

19,000 employees personal information and banking details compromised

hotels.ca



at&t

So did these people...

citigroup

3.9 Million Card & PIN Combos stolen

Honeywell

19,000 employees personal information and banking details compromised

Personal information on 243,000 customers exposed

hotels.ca

at&t

So did these people...



3.9 Million Card & PIN Combos stolen



19,000 employees personal information and banking details compromised

Personal information on 243,000 customers exposed



AT&T try to collect bills from the victims of hackers while they had been aware of the vulnerability of their system for over 10 years



And now the world knows....

- Do a quick google search
- CNN have an article “So your employer ‘lost’ your information
- If the US department of Veteran Affairs can have a laptop stolen with millions of names, birth dates and Social Security numbers on it, what sensitive information do you have on your company laptops that need protecting?
- The California “Security Breach Information Act (S.B. 1386)” requires companies that do business in California or that have customers in the state to notify consumers whenever their personal information may have been compromised. The California law exempts personal information that a company has stored in an encrypted format.

How does my static password breakdown?

- easy to guess
  andrina, admin, apple, password

- easy to crack
  AnDrInA, @dm1n etc...

- hard to remember
  @~D|/]^a! (yes, my name is in there somewhere...)

How does my static password breakdown?

- easy to guess
  andrina, admin, apple, password

- easy to crack
  AnDrInA, @dm1n etc...

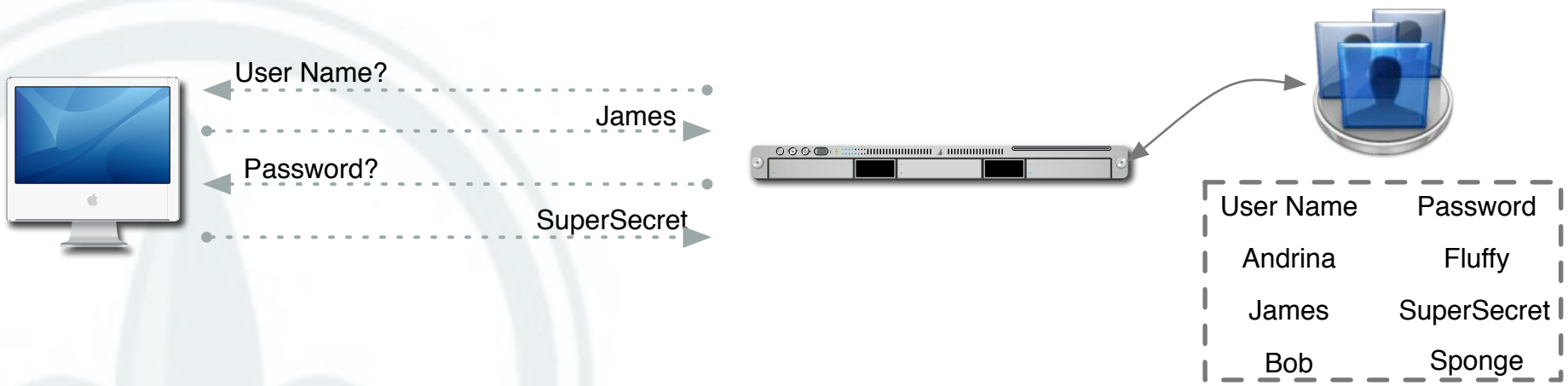
- hard to remember
  @~D|/]^a! (yes, my name is in there somewhere...)



Static Password Authentication

- The most basic form of authentication

- For a user to authenticate the user needs two things;
  identification or user name
  proof of identity with a password



There's a few more problems to solve...

- Identity theft is a global problem
- Government is mandating solutions (HIPPA, SOX etc...)
- Data Integrity
- Privileged & Confidential Information
- Falsified and Invalid Transactions

Ideally we're looking for something that...

- will authenticate users
- can't be stolen, sniffed, shoulder surfed or written down
- is actually going to be used by end users
- is not going to make the sys admin's head burst...

Why is 2 Factor Authentication any different?

2 Factor is a combination of proving who you are



What you have



What you know



Who you are

You've probably used 2 factor before...





You've probably used 2 factor before...



Where’s the benefit in this?

- Passwords can’t be shared, stolen, forgotten or written down
- If you lose one portion of your authentication, it’s useless to someone else
- You’ll (hopefully!) notice fairly soon that the physical part of your authentication is missing, unlike a stolen password

And how is this going to fit into my existing network?

- The workforce is moving more and more mobile
- People are working from home, from coffee shop hotspots, client offices, and even competitor's offices
- More and more of our everyday tools are moving into online assets
- 2 Factor Authentication is perfect for protecting VPN and web based portals

A quick look at an alternative....



Smart Cards

- Defined as any pocket-sized card with embedded integrated circuits
- We’re interested in their use for Public Key Infrastructure (PKI)
- The card will hold an encrypted digital signature issued from the PKI along with any other relevant information

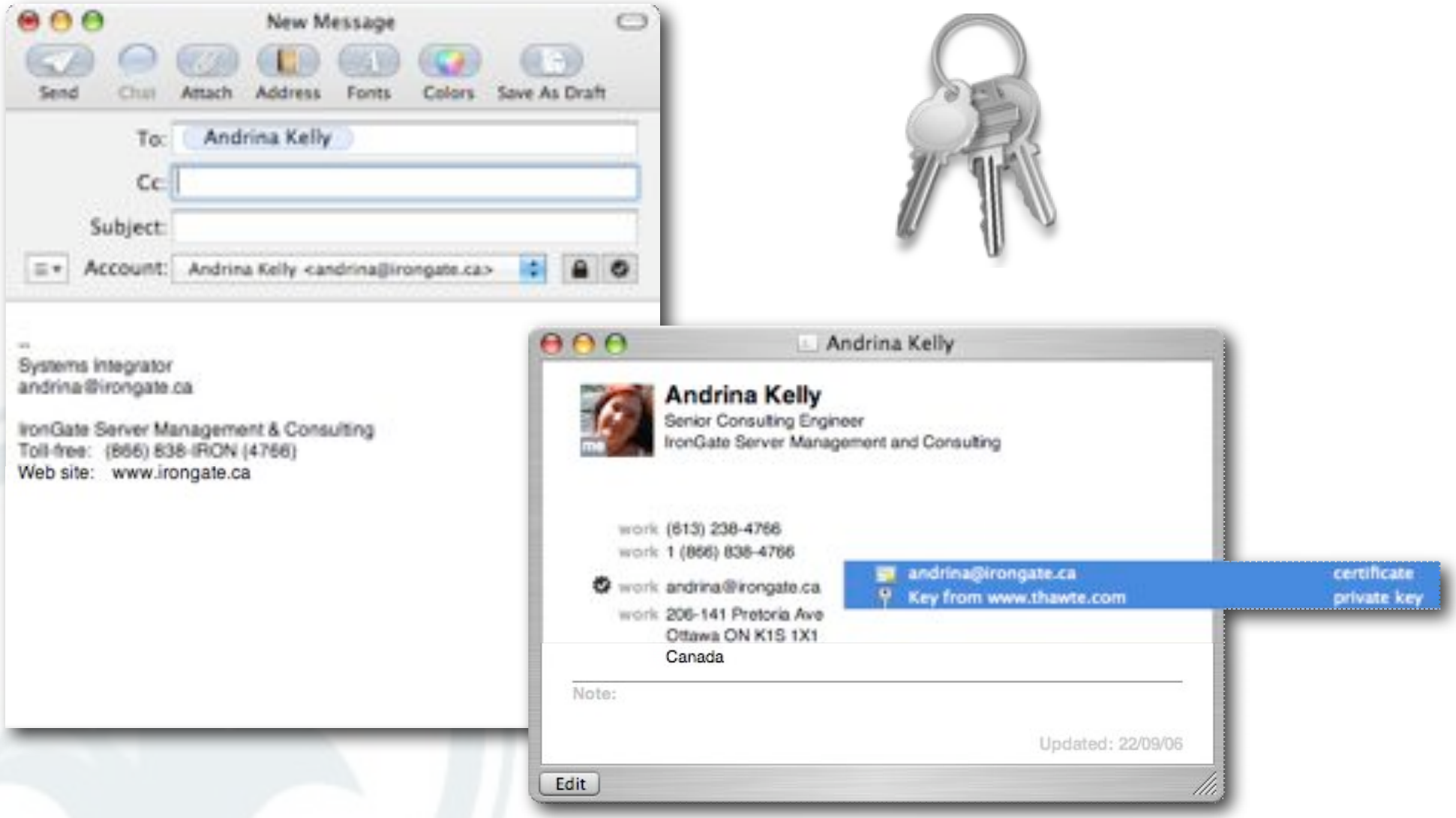


Typically held on a PKI-based Smart Card

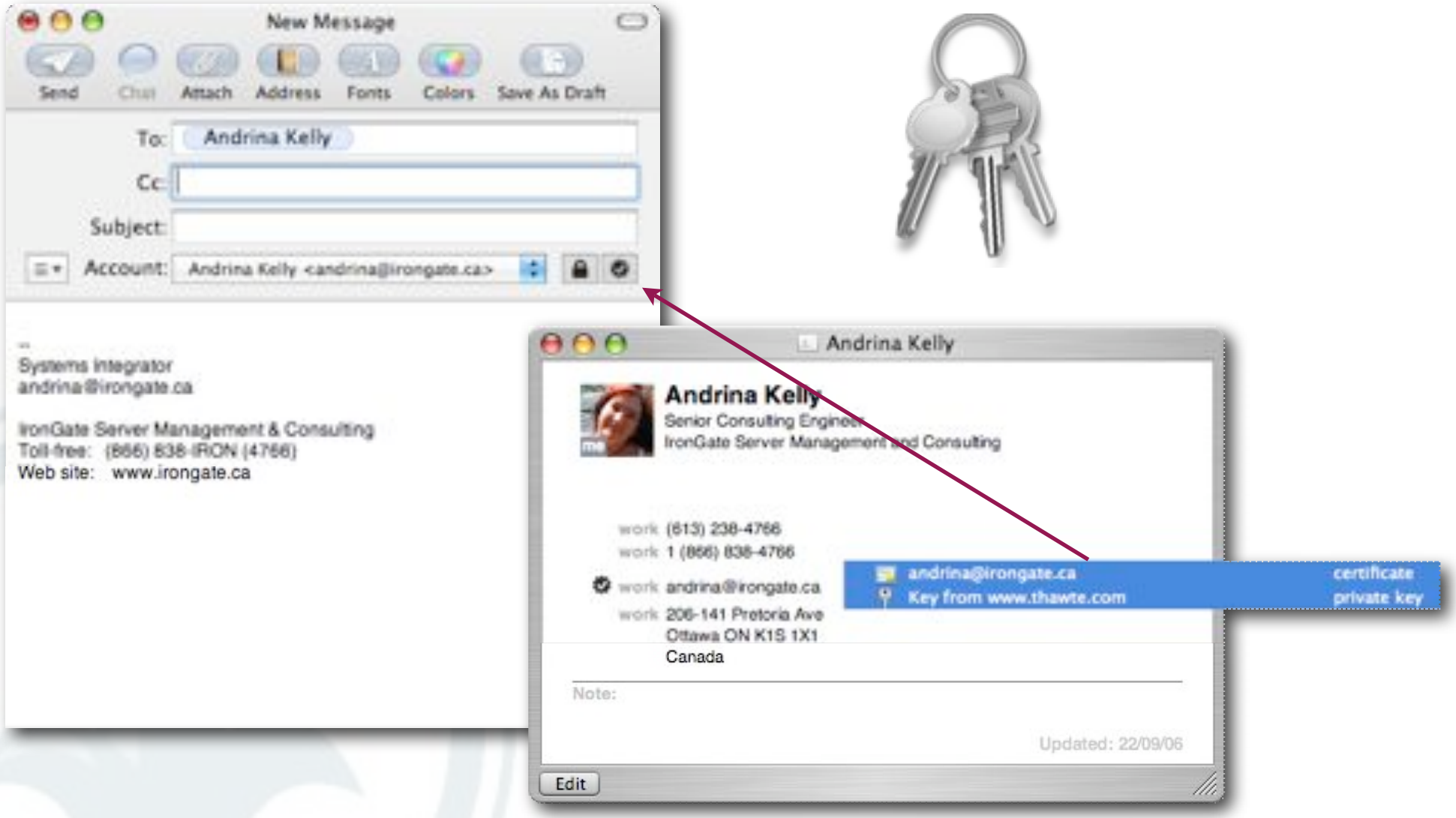
- Identity private key / public certificate
- E-mail signing private key / public certificate
- E-mail encryption private key / public certificate



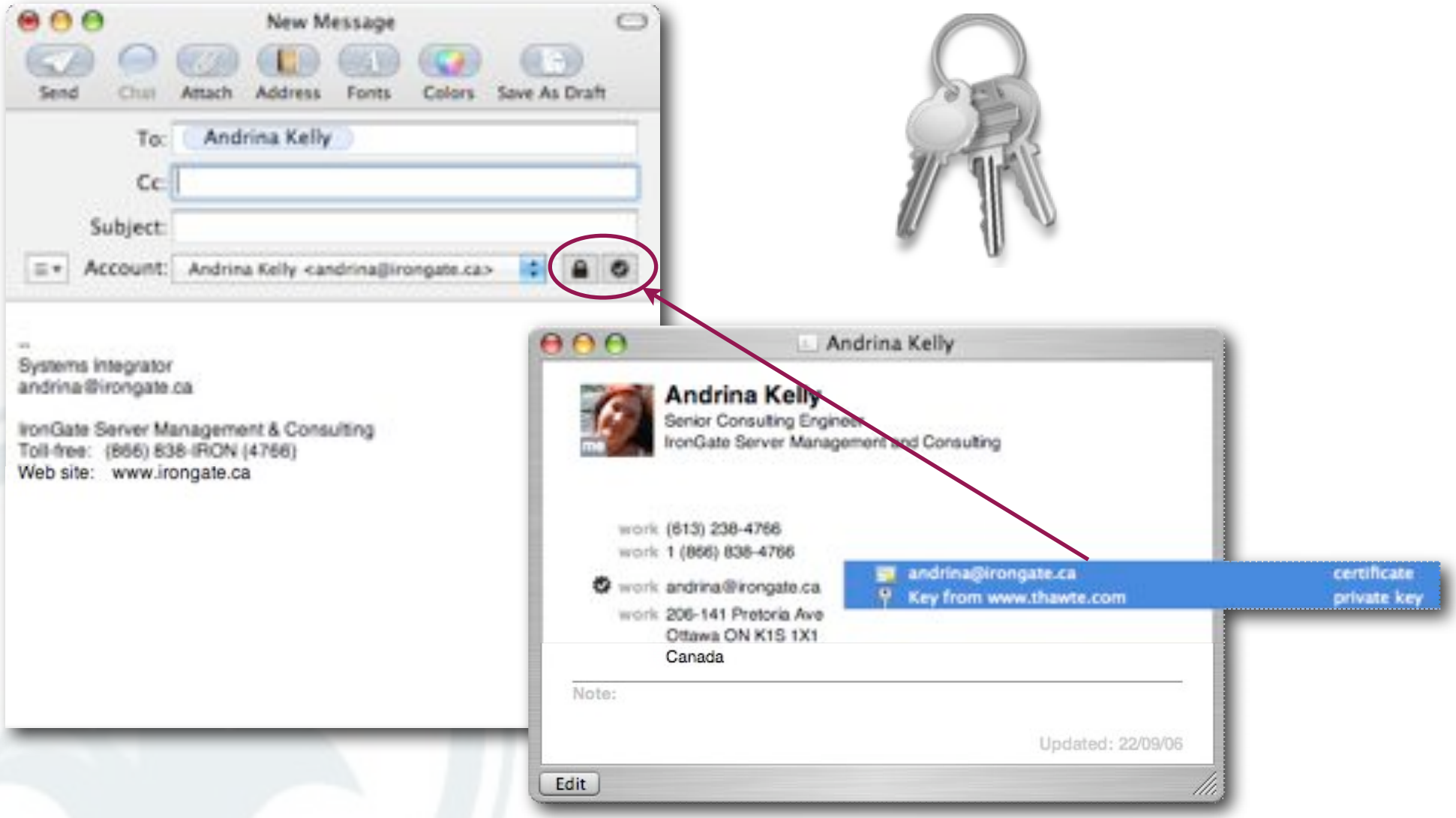
E-mail certificates in action...



E-mail certificates in action...



E-mail certificates in action...



Can also be used with...



Can also be used with...



Can also be used with...



Can also be used with...



Some slight tweaking is required...

modifying the right in /etc/authorization

```
<key>system.login.console</key>
<dict>
<key>class</key>
<string>evaluate-mechanisms</string>
<key>mechanisms</key>
<array>
<string>builtin:auto-login,privileged</string>
<string>loginwindow_builtin:login</string>
<string>builtin:reset-password,privileged</string>
<string>authinternal</string>
<string>builtin:getuserinfo,privileged</string>
<string>builtin:sso,privileged</string>
<string>HomeDirMechanism:login,privileged</string>
<string>HomeDirMechanism:status</string>
<string>MCXMechanism:login</string>
<string>loginwindow_builtin:success</string>
<string>loginwindow_builtin:done</string>
</array>
</dict>
```

Some slight tweaking is required...

modifying the right in /etc/authorization

```
<key>system.login.console</key>
<dict>
<key>class</key>
<string>evaluate-mechanisms</string>
<key>mechanisms</key>
<array>
<string>builtin:auto-login,privileged</string>
<string>loginwindow_builtin:login</string>
<string>builtin:reset-password,privileged</string>
<string>authinternal</string>
<string>builtin:getuserinfo,privileged</string>
<string>builtin:sso,privileged</string>
<string>HomeDirMechanism:login,privileged</string>
<string>HomeDirMechanism:status</string>
<string>MCXMechanism:login</string>
<string>loginwindow_builtin:success</string>
<string>loginwindow_builtin:done</string>
</array>
</dict>
```

Some slight tweaking is required...

modifying the right in /etc/authorization

```
<key>system.login.console</key>
<dict>
<key>class</key>
<string>evaluate-mechanisms</string>
<key>mechanisms</key>
<array>
<string>builtin:auto-login,privileged</string>
<string>builtin:smartcard-sniffer,privileged</string>
<string>loginwindow_builtin:login</string>
<string>builtin:reset-password,privileged</string>
<string>authinternal</string>
<string>builtin:getuserinfo,privileged</string>
<string>builtin:sso,privileged</string>
<string>HomeDirMechanism:login,privileged</string>
<string>HomeDirMechanism:status</string>
<string>MCXMechanism:login</string>
<string>loginwindow_builtin:success</string>
<string>loginwindow_builtin:done</string>
</array>
</dict>
```

Some slight tweaking is required...

modifying the rule in /etc/authorization

```
<key>authenticate</key>
<dict>
<key>class</key>
<string>evaluate-mechanisms</string>
<key>mechanisms</key>
<array>
<string>builtin:authenticate</string>
<string>authinternal</string>
</array>
</dict>
```

Some slight tweaking is required...

modifying the rule in /etc/authorisation

```
<key>authenticate</key>
<dict>
<key>class</key>
<string>evaluate-mechanisms</string>
<key>mechanisms</key>
<array>
<string>builtin:authenticate</string>
<string>authinternal</string>
</array>
</dict>
```

Some slight tweaking is required...

modifying the rule in /etc/authorisation

```
<key>authenticate</key>
<dict>
<key>class</key>
<string>evaluate-mechanisms</string>
<key>mechanisms</key>
<array>
<string>builtin:smartcard-sniffer,privileged</string>
<string>builtin:authenticate</string>
<string>authinternal</string>
<string>builtin:authenticate,privileged</string>
</array>
</dict>
```

Further Resources

- Apple kbase #304035 “Enabling Smart Card Login” - this also shows setting up Smart Card authentication for LDAP based users.

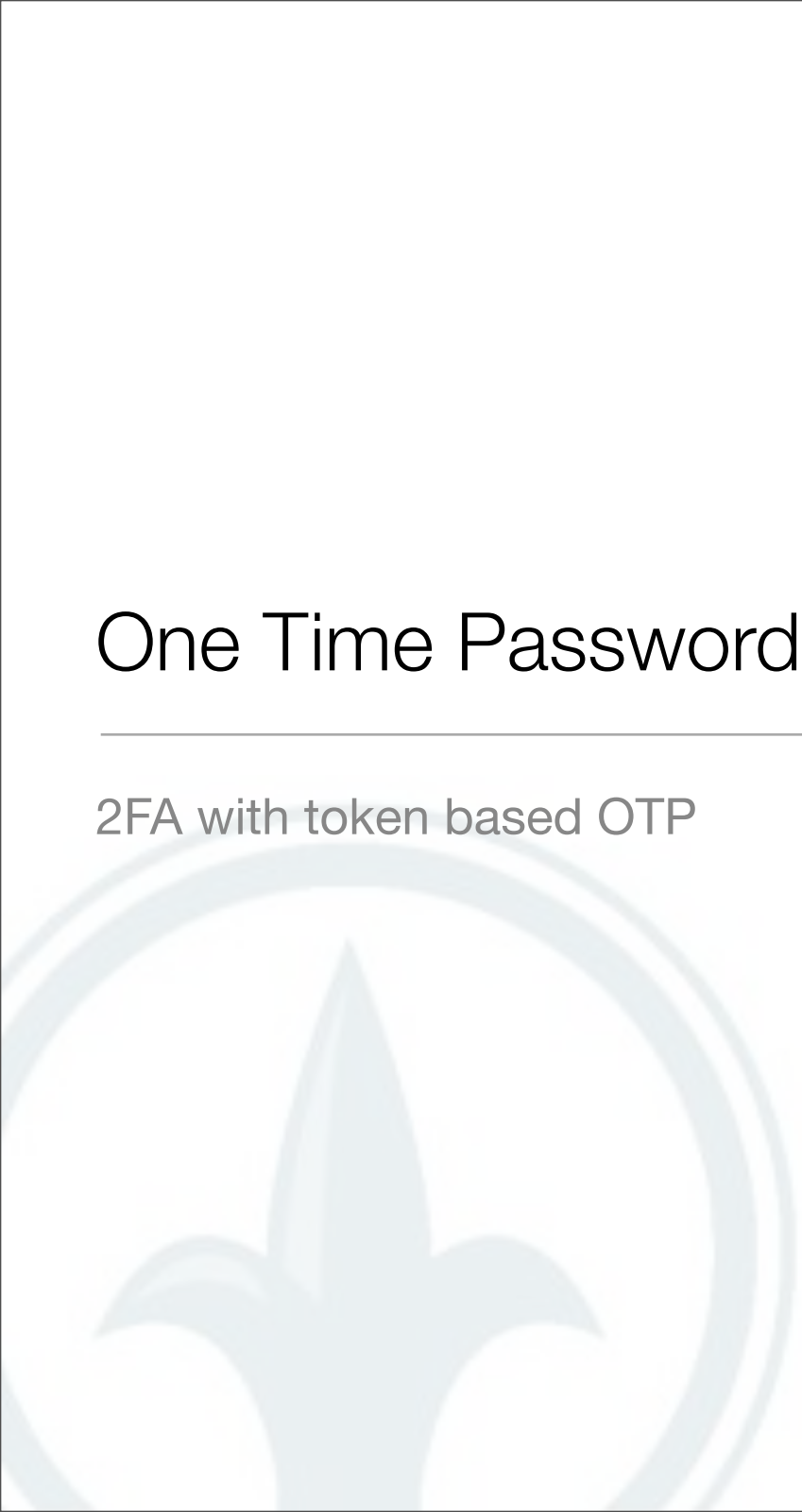
- Apple kbase #25526 “Apple Federal Smart Card Package Installation and Setup Guide” - slightly outdated now, but still good information

- OpenSC - http://www.opensc-project.org/sca - OpenSC provides a set of libraries and utilities to access smart cards. OpenSC implements the PKCS#11 API so applications supporting this API such as Mozilla Firefox and Thunderbird can use it. OpenSC implements the PKCS#15 standard and aims to be compatible with every software that does so, too.

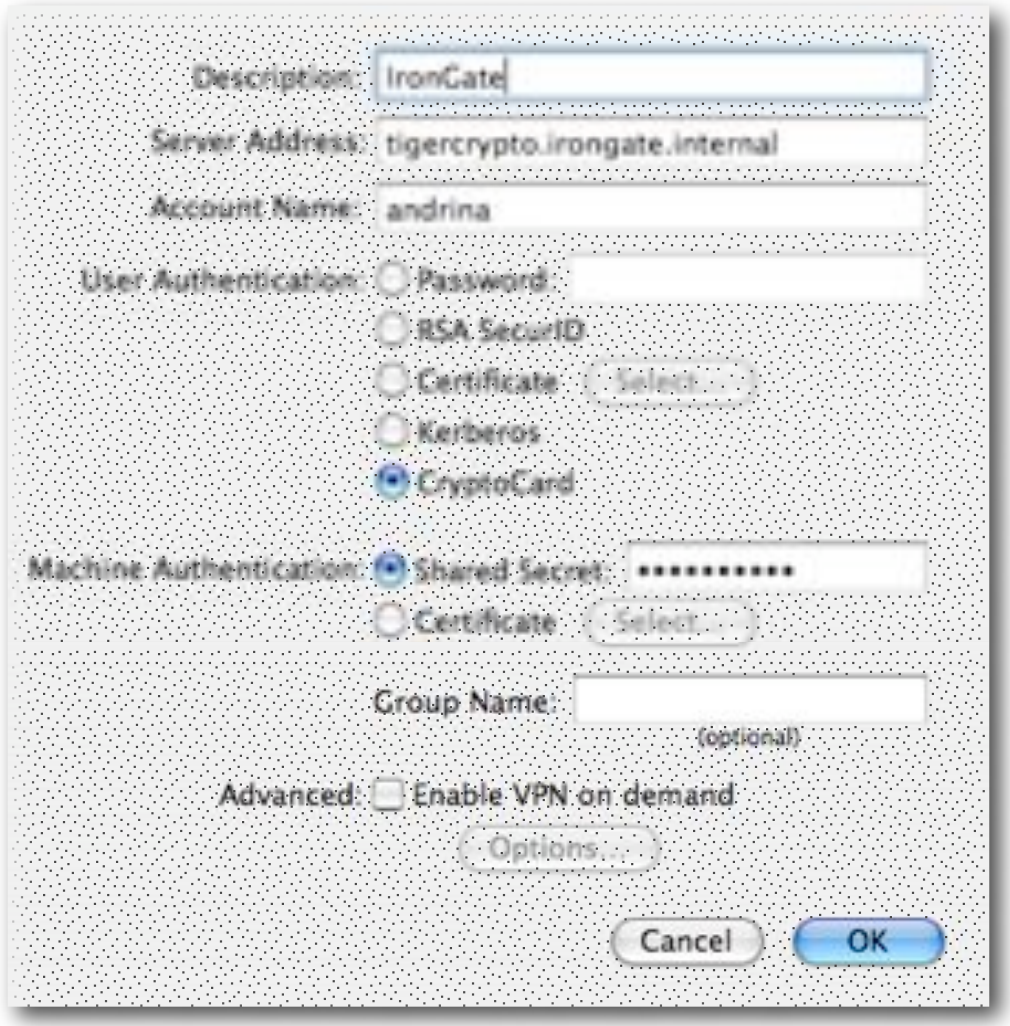
- ADC - http://developer.apple.com/documentation/Security/Conceptual/SecureCodingGuide/Articles/SecuritySvcs.html

One Time Passwords

2FA with token based OTP

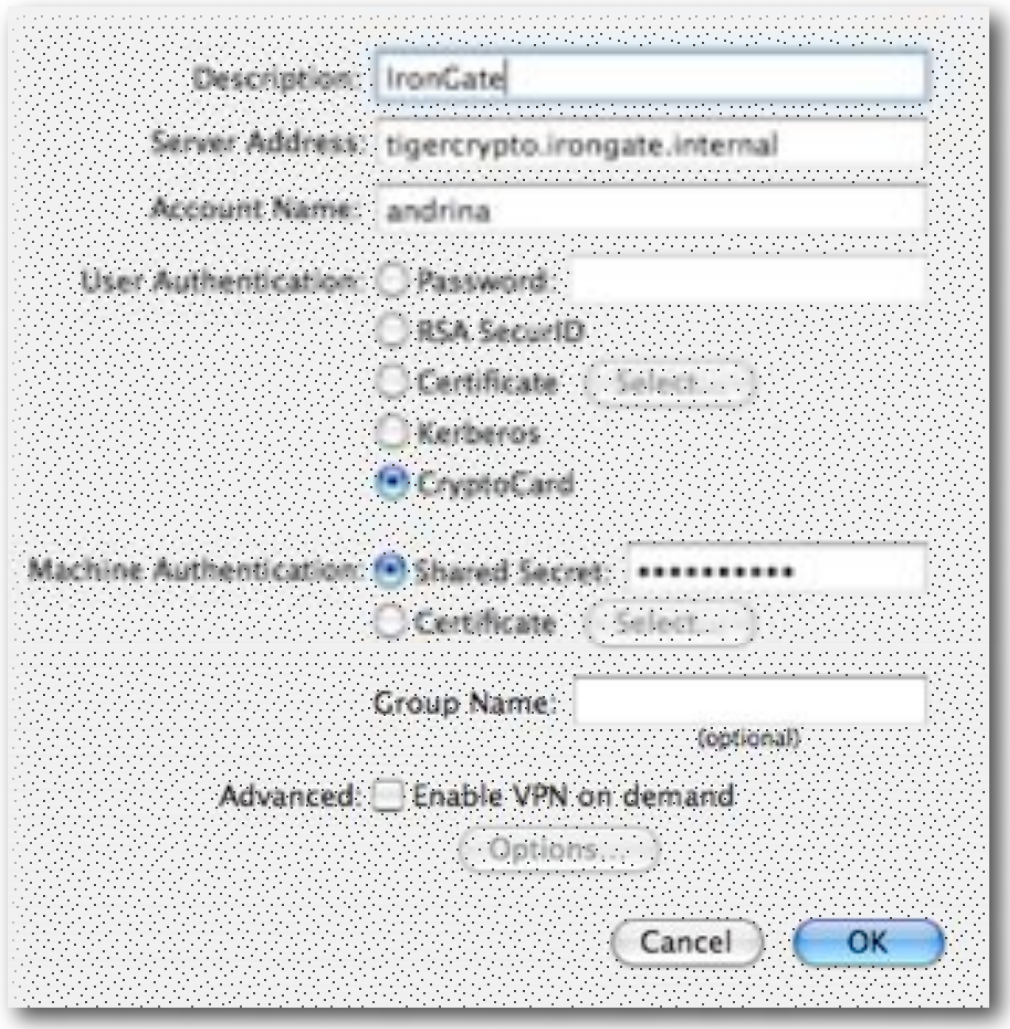


OTP Support is built-in



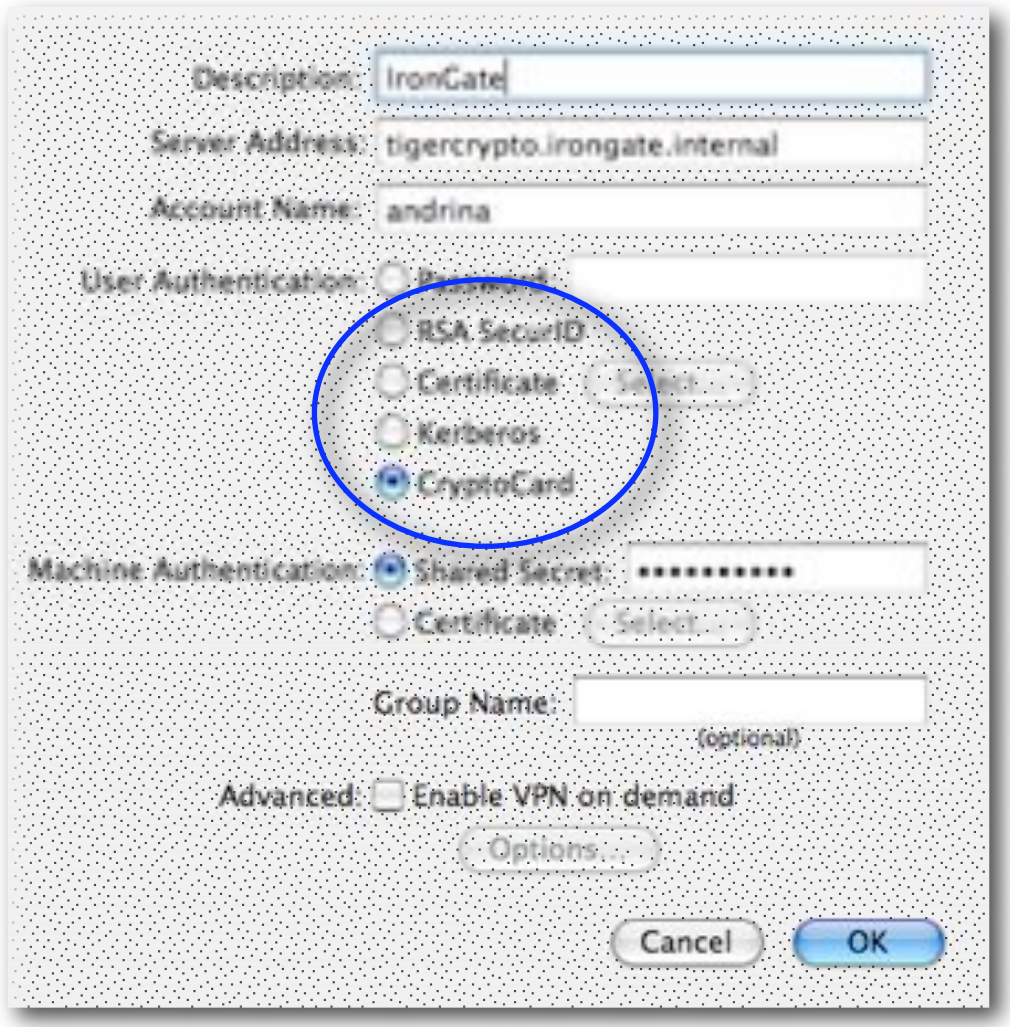
OTP Support is built-in

- Support for both RSA SecureID and CRYPTOCard are built in
- No CLI modifications required



OTP Support is built-in

- Support for both RSA SecureID and CRYPTOCard are built in
- No CLI modifications required



So, how is CRYPTOCard different to Smart Cards?

CRYPTO-Server

- Central brain for authentication
- All login attempts are passed through the CRYPTO-Server
- All login activity is also logged
- Supports a number of protocols
- Includes failover/redundancy functionality

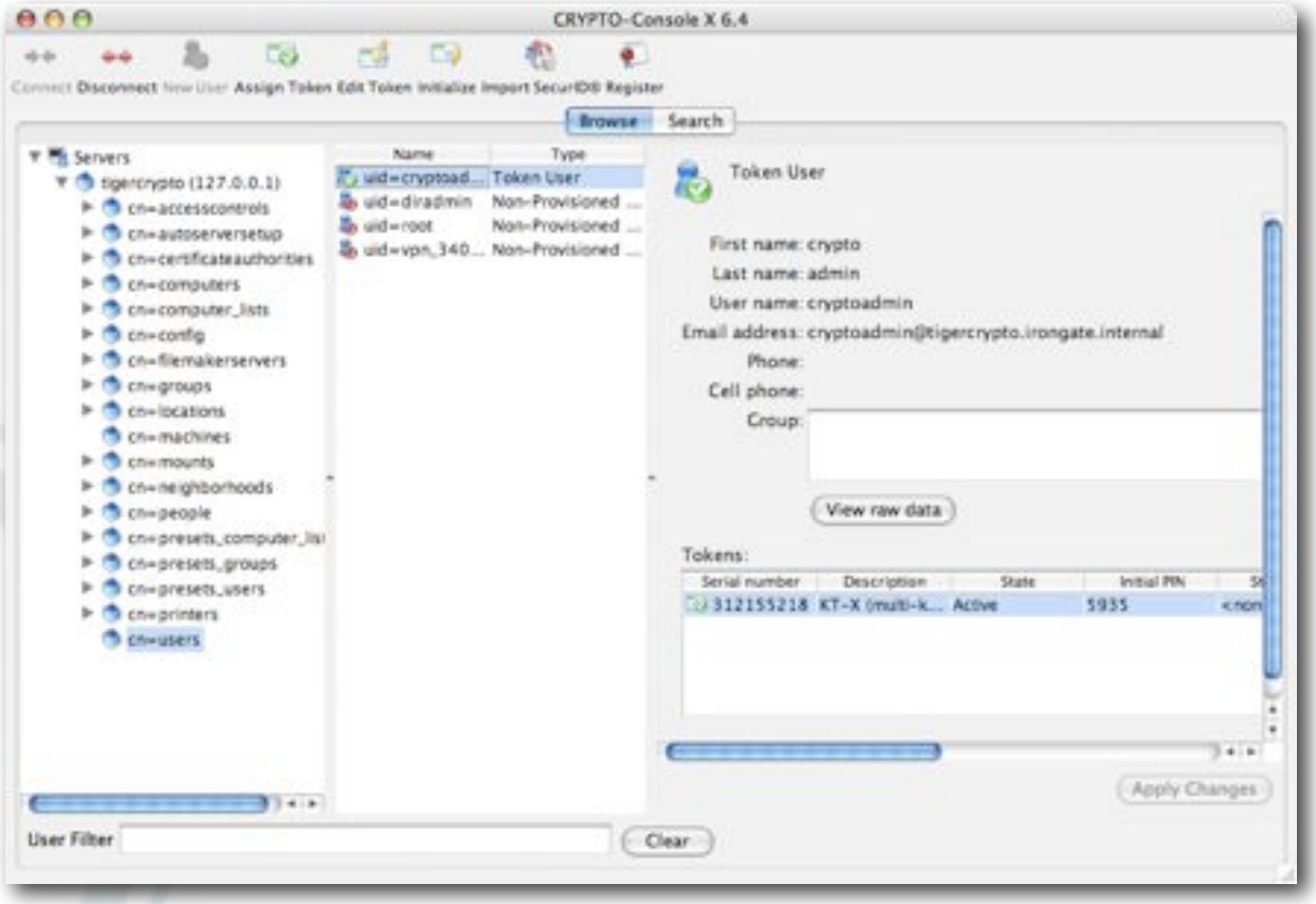


Practical Applications

- VPN access - Internet Connect
- Network Authentication - CRYPTO-Logon
- Web Access - CRYPTO-Web

CRYPTO-Console

- Used for token management
- Server Licensing
- Reporting functions



Lots of variety in the tokens...









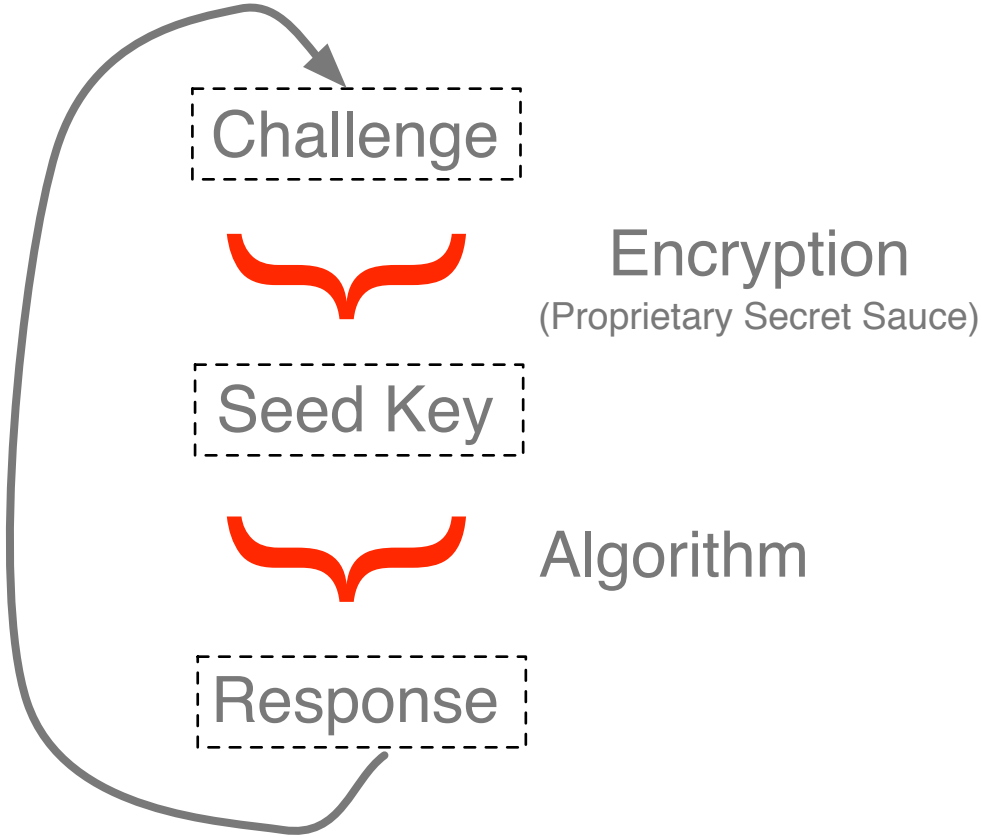
What is a Token?

- All All tokens use encryption techniques to generate One-time passwords. The concept is quite simple.
- By passing a known value, sometimes referred to as a "Challenge" through an encryption algorithm to create the “SEED KEY”.
- Taking the “SEED KEY” and using it against an algorithm to calculate the response is derived using either DES, 3DES, AES-128, AES-192 or AES-256 algorithms.



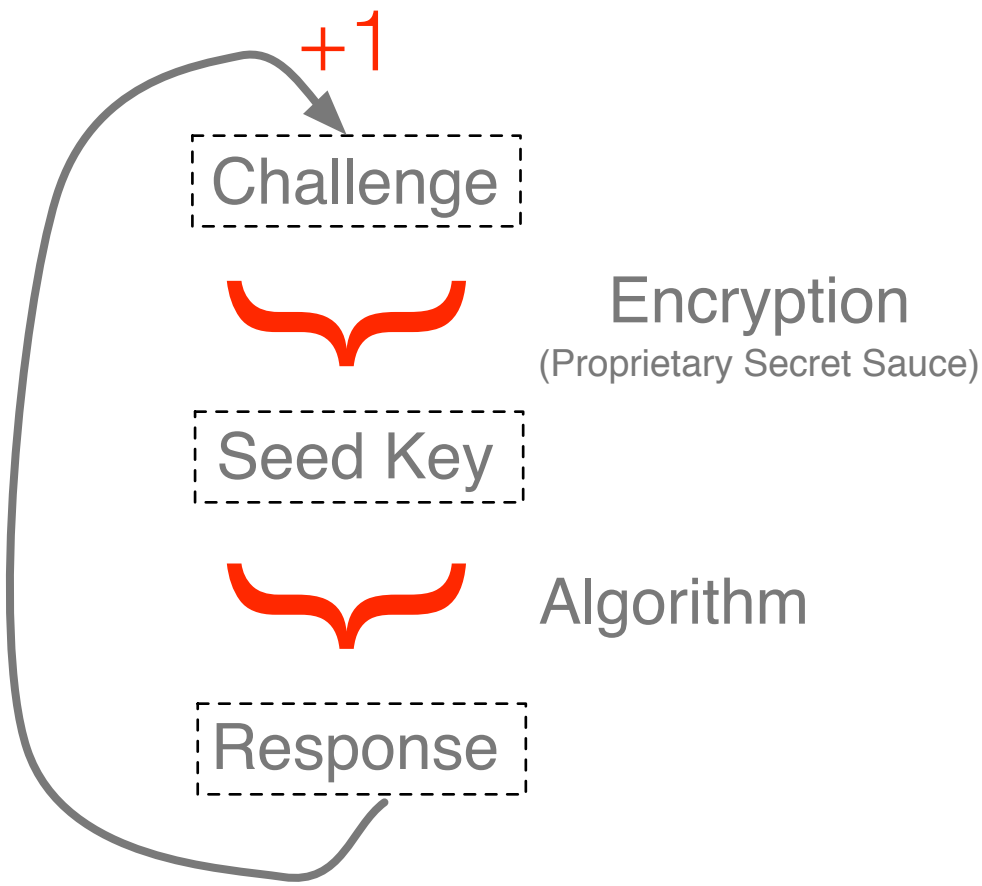
What is a Token?

- All All tokens use encryption techniques to generate One-time passwords. The concept is quite simple.
- By passing a known value, sometimes referred to as a "Challenge" through an encryption algorithm to create the “SEED KEY”.
- Taking the “SEED KEY” and using it against an algorithm to calculate the response is derived using either DES, 3DES, AES-128, AES-192 or AES-256 algorithms.

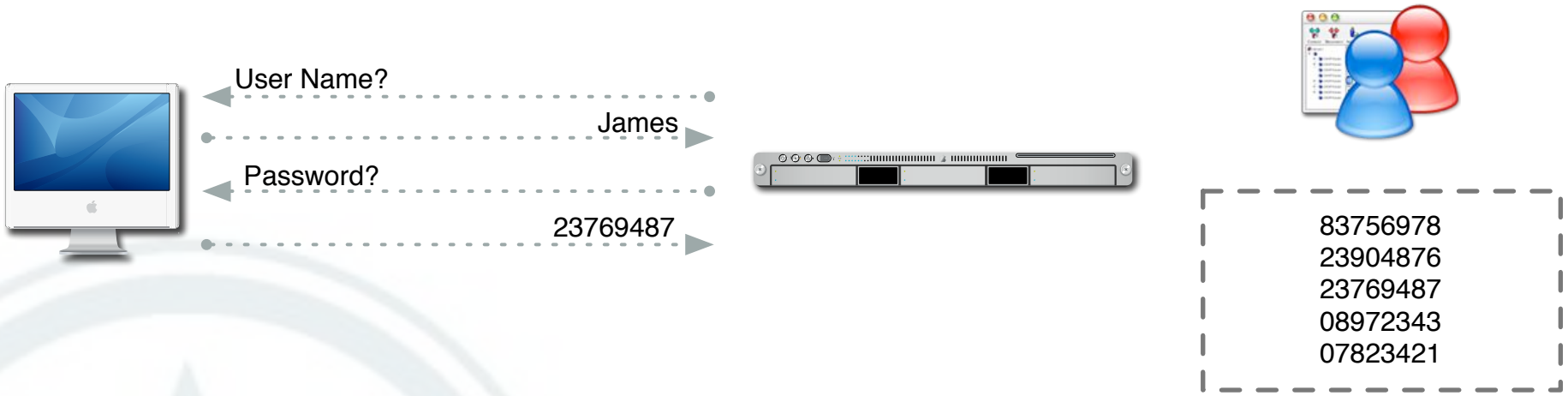


What is a Token?

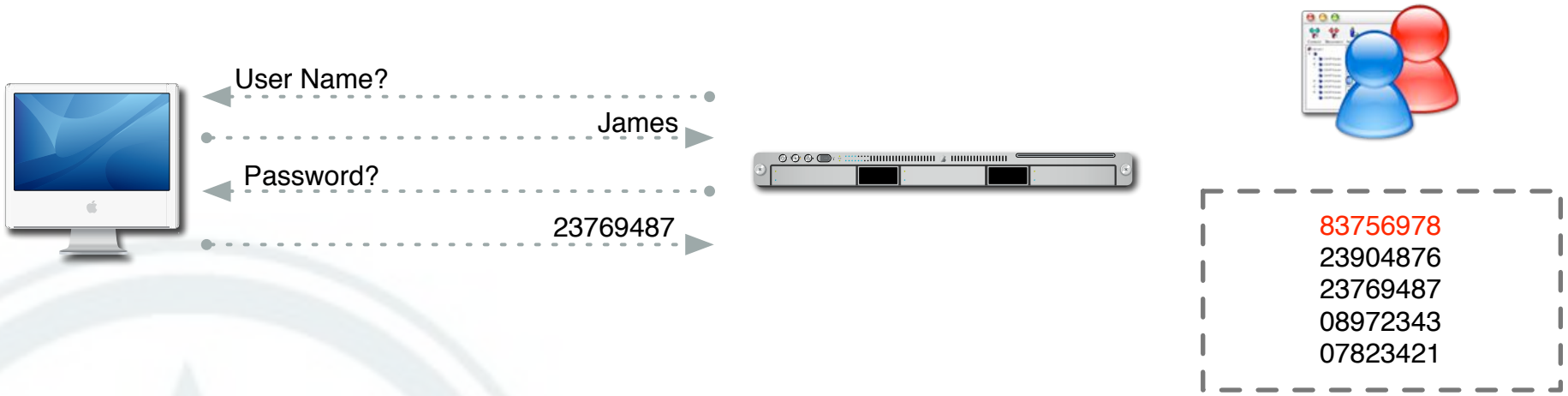
- All All tokens use encryption techniques to generate One-time passwords. The concept is quite simple.
- By passing a known value, sometimes referred to as a "Challenge" through an encryption algorithm to create the “SEED KEY”.
- Taking the “SEED KEY” and using it against an algorithm to calculate the response is derived using either DES, 3DES, AES-128, AES-192 or AES-256 algorithms.



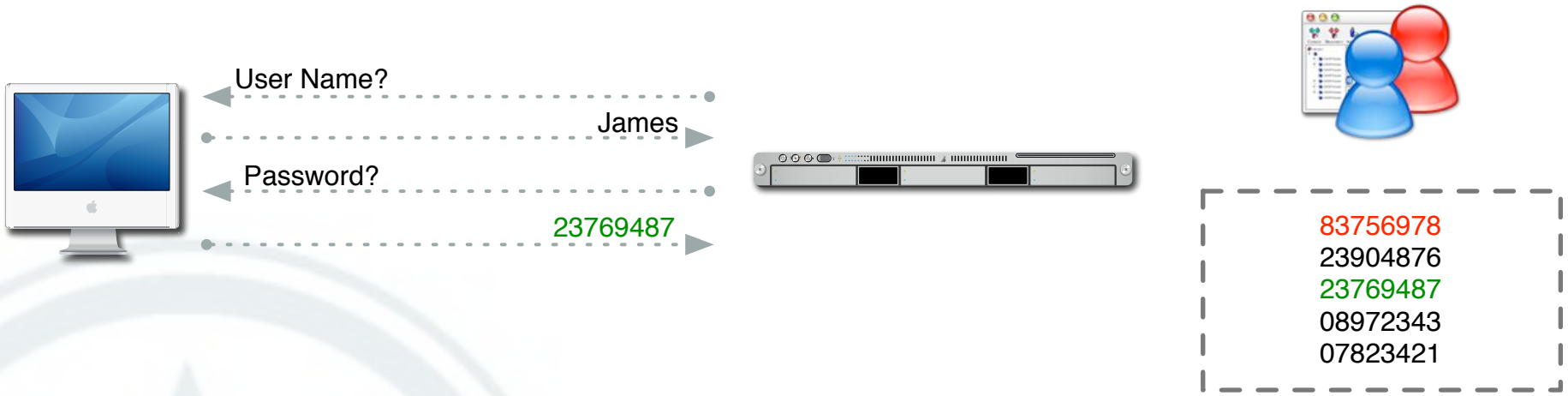
Event Synchronous Tokens



Event Synchronous Tokens



Event Synchronous Tokens



Token Features

- Complexity can be handled by the token - allowing the user to have an easier password to remember
- Start/Stop Dates - for temporary workers, once the contract is over the token is disabled
- Integrates easily into existing directory structure - no need to enter user details twice

Username Repository

- Provides authentication for users stored in Active Directory, Open LDAP, Open Directory, or the CRYPTO-Card installed MySQL database

- The username repository is a read-only connection

Token Repository

- CRYPTOCard tokens are held in either the default MySQL database or in the optional MS-SQL or Oracle databases
- In the case of Active Directory, the Microsoft UID number is used to associate to the username within the Token Repository

3rd Party Integration

- Based on RADIUS
- Interoperability with other hardware appliances (Cisco, Juniper etc.)

CRYPTO-Web Setup Demo

Just how easy is easy...



Demo Recap

- Ensure you have a server with a fully qualified domain - check your forward and reverse DNS
- Remember the admin PIN!
- Create a secondary CRYPTO-Console administrative user
- If you are going to use hardware tokens, ensure you have a working internet connection for registration
- When setting up the security on your website, connect to CRYPTO-Web from a remote machine - i.e. not your CRYPTO-Server

CRYPTO-VPN Setup Demo

Let’s break out of the GUI, but it’s still a 10 minute job...

Demo Recap

- Ensure you have a working Apple VPN solution with static passwords first.
- Backup and make your changes to com.apple.RemoteAccessServers.plist
- Create your /etc/ppp/postoptions file
- Restart the CRYPTO Protocol Server
- Stay away from the VPN GUI in Server Admin (as it it were a swarm of bees...)
- No modifications required outside of Internet Connect on the client end

Q & A