

Beyond files forensic

OWADE cloud based forensic

Elie Bursztein *Stanford University*

Ivan Fontarensky *Cassidian*

Matthieu Martin *Stanford University*

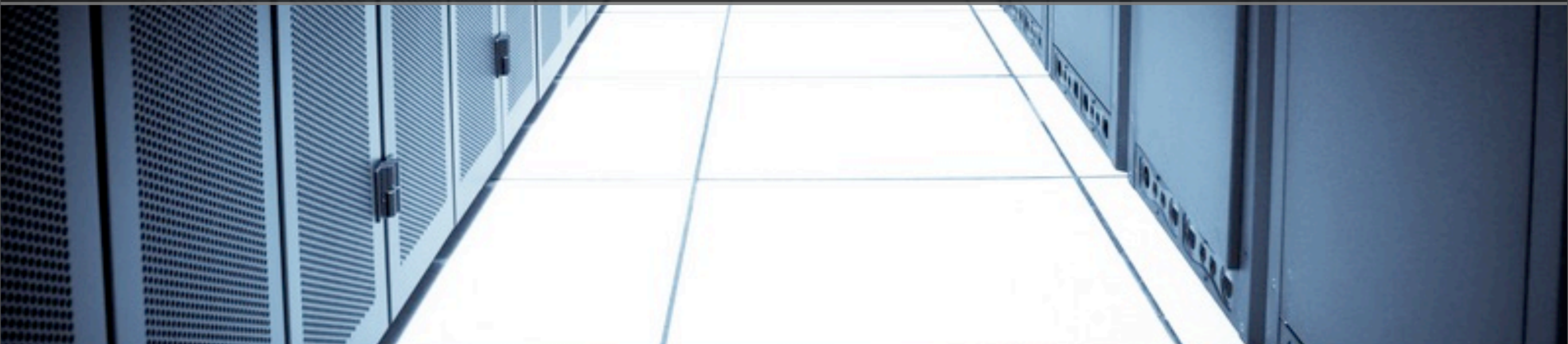
Jean Michel Picod *Cassidian*



福



The world is moving to the **cloud**



A close-up, slightly blurred photograph of a computer monitor. The word "facebook" is visible in white lowercase letters on a dark blue rectangular background, which is part of the Facebook logo. The rest of the screen and the surrounding environment are out of focus.

facebook

2.7 millions photos are uploaded to Facebook
every **20 minutes**

A close-up, slightly blurred photograph of a computer screen. The word "password" is visible in a dark font, likely serving as a label for a password input field. The rest of the screen is out of focus.

password



100 millions new files are saved on Dropbox
every **day**

Data are moving to multiple services

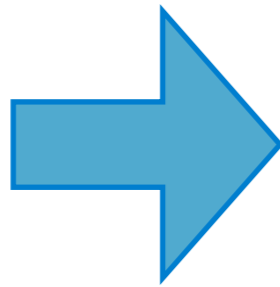


Hard drive

Data are moving to multiple services



Hard drive

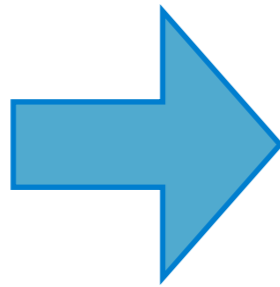


emails

Data are moving to multiple services



Hard drive



emails

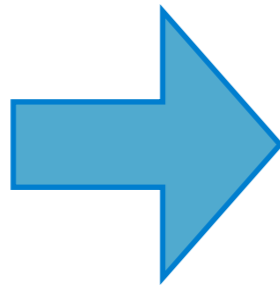


Cloud

Data are moving to multiple services



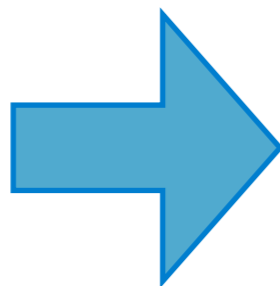
Hard drive



emails



Cloud

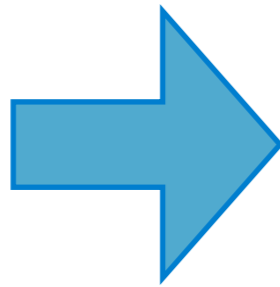


Webmail

Data are moving to multiple services



Hard drive



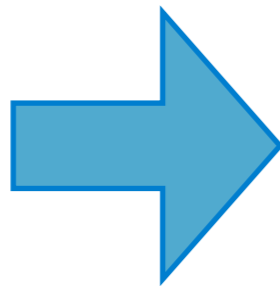
emails



contacts



Cloud

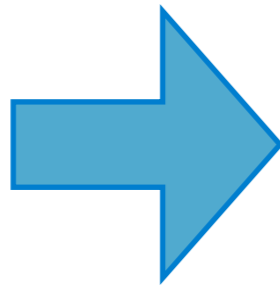


Webmail

Data are moving to multiple services



Hard drive



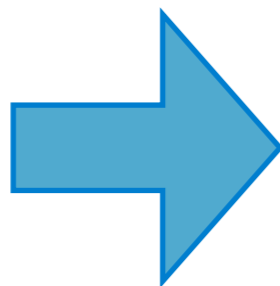
emails



contacts



Cloud



Webmail

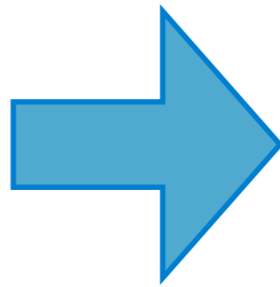


Social sites

Data are moving to multiple services



Hard drive



emails



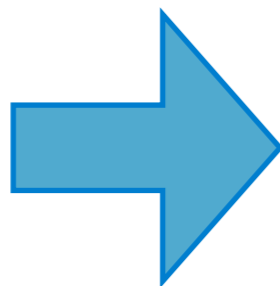
contacts



photos



Cloud



Webmail

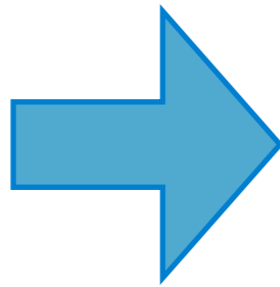


Social sites

Data are moving to multiple services



Hard drive



emails



contacts

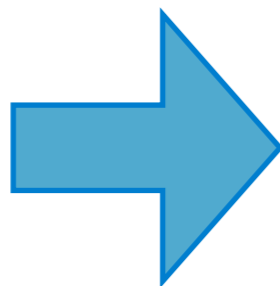


photos



Photo sites

Cloud



Webmail

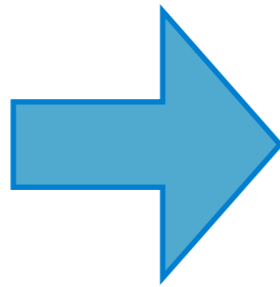


Social sites

Data are moving to multiple services



Hard drive



emails



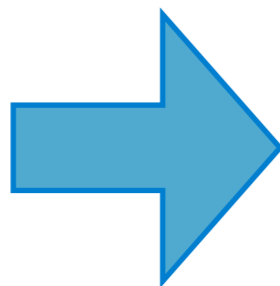
contacts



photos



Cloud



Webmail



Social sites



Photo sites

Impact on the forensic field

- There are **more** data which are **harder** to reach
- Dealing with **cloud data** force us to **reinvent** forensic



The background of the slide is a close-up of red, pleated curtains. The top part of the image shows the curtains gathered at the top, with a large, curved valance. Below this, the curtains hang in deep, vertical folds, creating a rhythmic pattern of light and shadow. The color is a rich, slightly dark red. A dark grey horizontal band is superimposed over the middle of the image, containing the main text.

Let's do **cloud** forensics



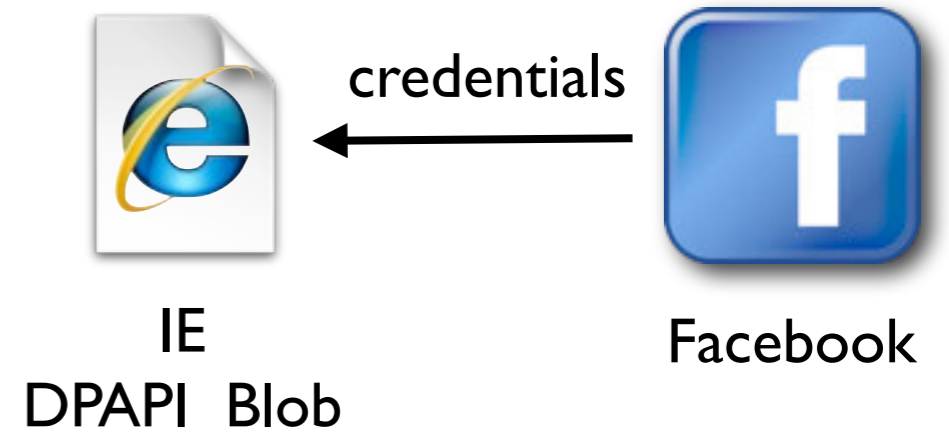
What is **cloud forensics** ?

Facebook credentials as a use case

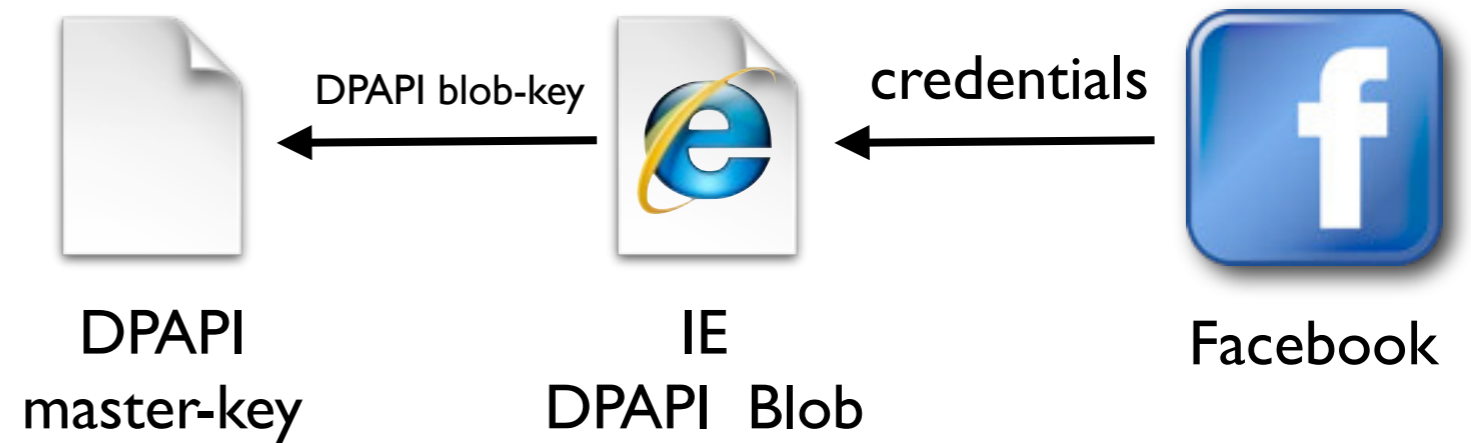


Facebook

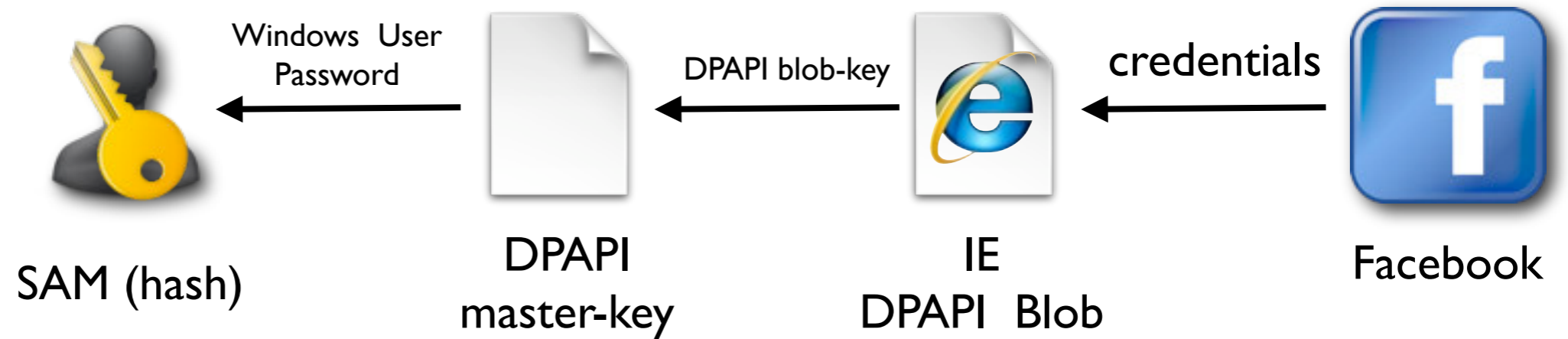
Facebook credentials as a use case



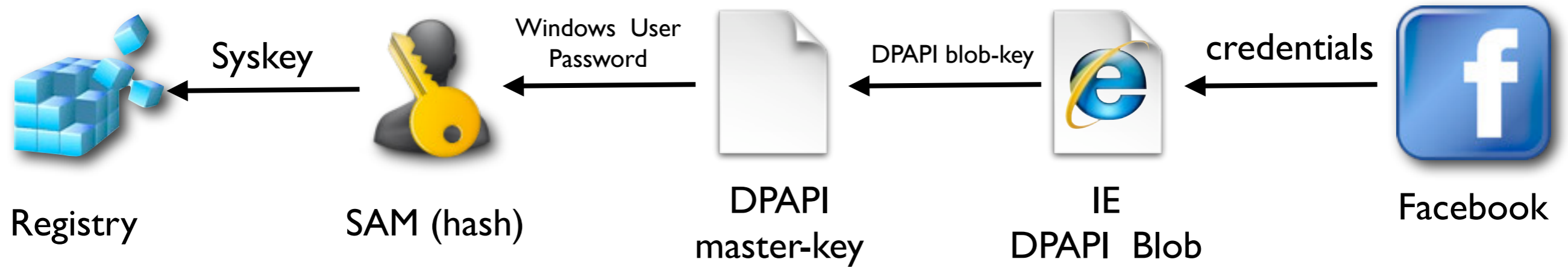
Facebook credentials as a use case



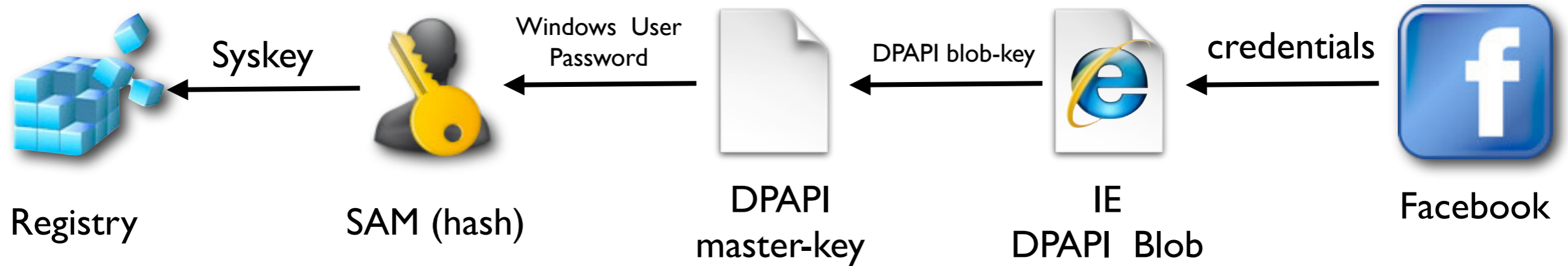
Facebook credentials as a use case



Facebook credentials as a use case



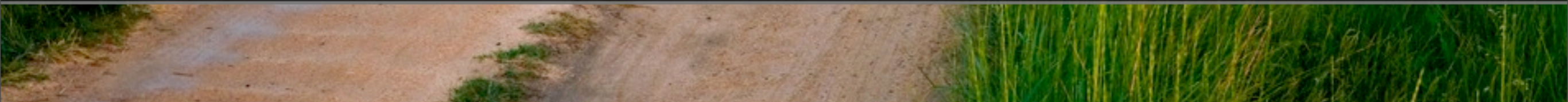
Facebook credentials as a use case



Getting Facebook credentials require to **bypass 4 layers of encryption**



Show you how to **bypass the encryption layers** and get
the data you want



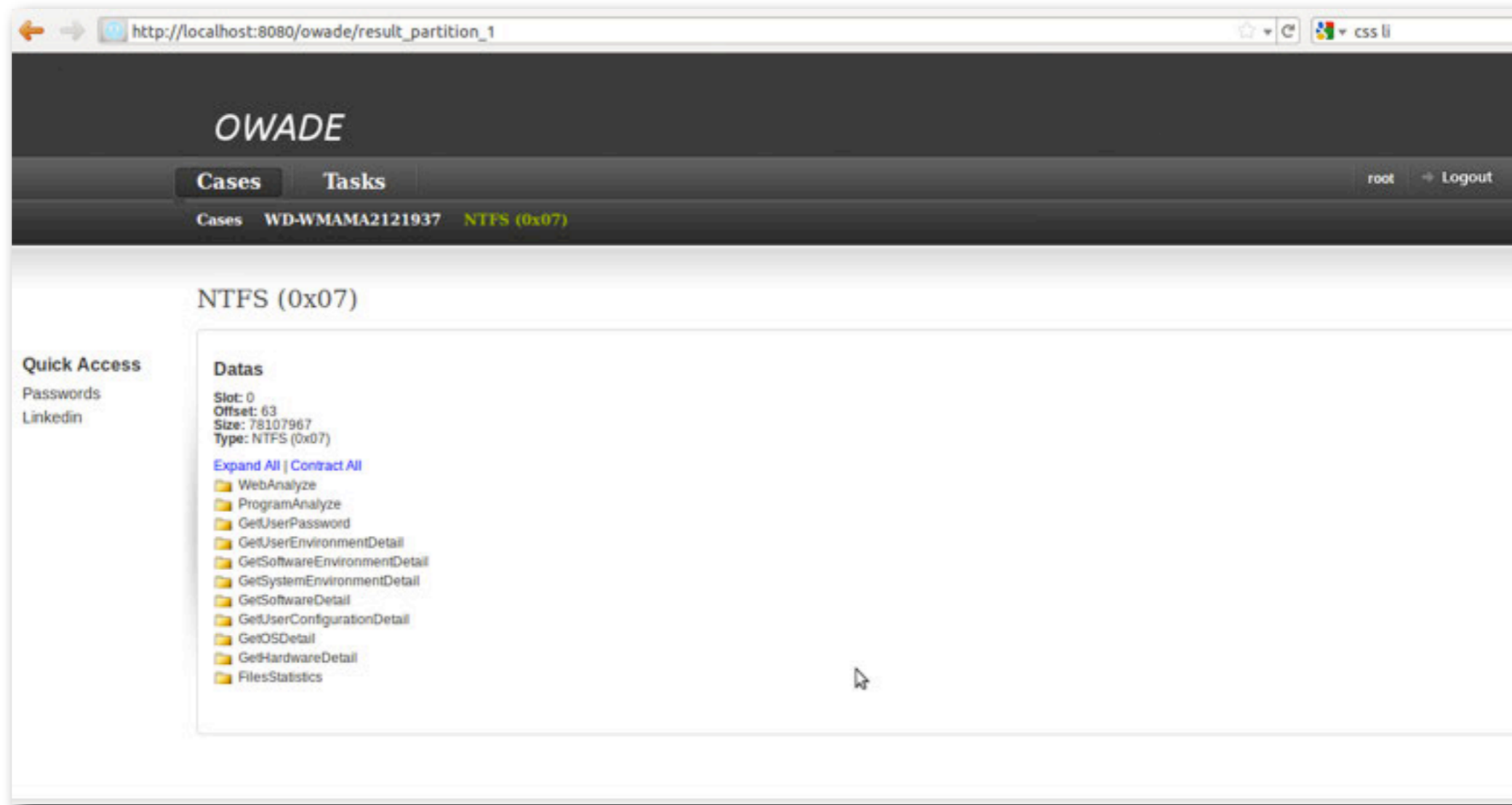
Introducing OWADE

- Dedicated to cloud forensics
- Decrypt / recovers
 - DPAPI secrets
 - Browsers history and websites credentials
 - Instant messaging creds
 - Wifi data
- Free and open-source



<http://owade.org>

OWADE in action



The screenshot shows a web browser window with the URL `http://localhost:8080/owade/result_partition_1`. The page title is "OWADE". The navigation bar includes "Cases" and "Tasks" tabs, and a user profile "root" with a "Logout" link. The main content area displays "Cases WD-WMAMA2121937 NTFS (0x07)". Below this, the section "NTFS (0x07)" is expanded to show a "Datas" section with the following details:

- Slot: 0
- Offset: 63
- Size: 78107967
- Type: NTFS (0x07)

Below the details are links for "Expand All" and "Contract All", followed by a list of data items:

- WebAnalyze
- ProgramAnalyze
- GetUserPassword
- GetUserEnvironmentDetail
- GetSoftwareEnvironmentDetail
- GetSystemEnvironmentDetail
- GetSoftwareDetail
- GetUserConfigurationDetail
- GetOSDetail
- GetHardwareDetail
- FilesStatistics

A "Quick Access" sidebar on the left contains links for "Passwords" and "Linkedin".



OWADE overview

OWADE overview



disk

OWADE overview



disk



disk image

OWADE overview



Registry



disk



disk image

OWADE overview



Registry



disk



disk image



Files

OWADE overview



Windows
credentials



Registry



disk



disk image



Files

OWADE overview



Windows
credentials



Registry



WiFi info



Files



disk



disk image

OWADE overview



Windows
credentials



Registry



WiFi info



Files



Hardware
info



disk



disk image

OWADE overview



disk



disk image



Registry



Files



Windows credentials



WiFi info



Hardware info



Credentials and data

OWADE overview



disk



disk image



Registry



Files



Windows credentials



WiFi info



Hardware info



Credentials and data



Cloud data

Outline

Outline

- **File base forensics refresher**

Outline

- File base forensics refresher
- The Windows crypto eco-system

Outline

- File base forensics refresher
- The Windows crypto eco-system
- Wifi data and Geo-location

Outline

- File base forensics refresher
- The Windows crypto eco-system
- Wifi data and Geo-location
- Recovering browser data

Outline

- File base forensics refresher
- The Windows crypto eco-system
- Wifi data and Geo-location
- Recovering browser data
- Recovering instant messaging data

Outline

- File base forensics refresher
- The Windows crypto eco-system
- Wifi data and Geo-location
- Recovering browser data
- Recovering instant messaging data
- Acquiring cloud data

Outline

- File base forensics refresher
- The Windows crypto eco-system
- Wifi data and Geo-location
- Recovering browser data
- Recovering instant messaging data
- Acquiring cloud data
- Demo

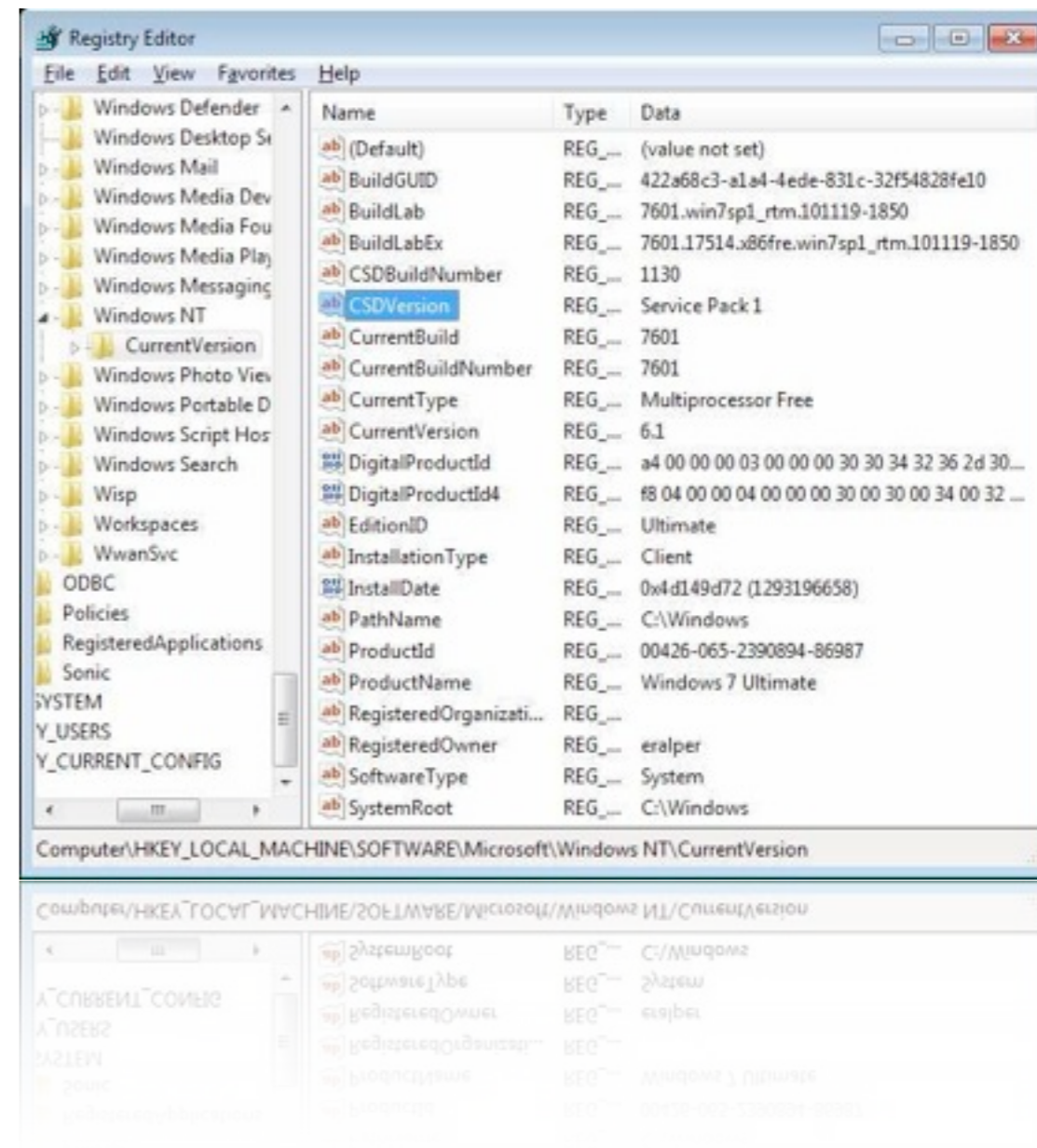
File based forensic refresher

Not all files are born equal

Type of file	how to recover it
Standard	copy
In the trash	undelete utility
Deleted	file carving
Wiped	call the NSA :)

Windows registry

- .dat files
- Hardware information
- Softwares installed with their versions and serials
- Windows credentials (encrypted)



Some Registry Information Extracted

type: registry (hex)

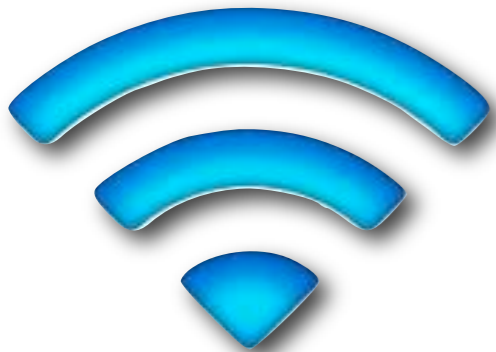
Expand All | Contract All

- WebAnalyze
- ProgramAnalyze
- GetUserPassword
- GetUserEnvironmentDetail
- GetSoftwareEnvironmentDetail
- GetSystemEnvironmentDetail
- GetSoftwareDetail
- GetUserConfigurationDetail
- GetOSDetail
- GetHardwareDetail
 - FDC
 - USBSTOR
 - FriendlyName1: Generic USB MS Reader USB Device
 - FriendlyName0: Generic USB CF Reader USB Device
 - FriendlyName3: Disk drive
 - FriendlyName2: Generic USB SD Reader USB Device
 - FriendlyName5: HP v100w USB Device
 - FriendlyName4: HP v100w USB Device
 - SW
 - ACPI
 - FriendlyName1: Intel(R) Core(TM) i7 CPU 920 @ 2.67GHz
 - FriendlyName0: Intel(R) Core(TM) i7 CPU 920 @ 2.67GHz
 - FriendlyName3: Intel(R) Core(TM) i7 CPU 920 @ 2.67GHz
 - FriendlyName2: Intel(R) Core(TM) i7 CPU 920 @ 2.67GHz
 - FriendlyName5: Intel(R) Core(TM) i7 CPU 920 @ 2.67GHz
 - FriendlyName4: Intel(R) Core(TM) i7 CPU 920 @ 2.67GHz
 - FriendlyName7: Intel(R) Core(TM) i7 CPU 920 @ 2.67GHz
 - FriendlyName6: Intel(R) Core(TM) i7 CPU 920 @ 2.67GHz
 - PCI
 - SCSI
 - IDE
 - PCIDE
 - DISPLAY
- FilesStatistics



Windows crypto

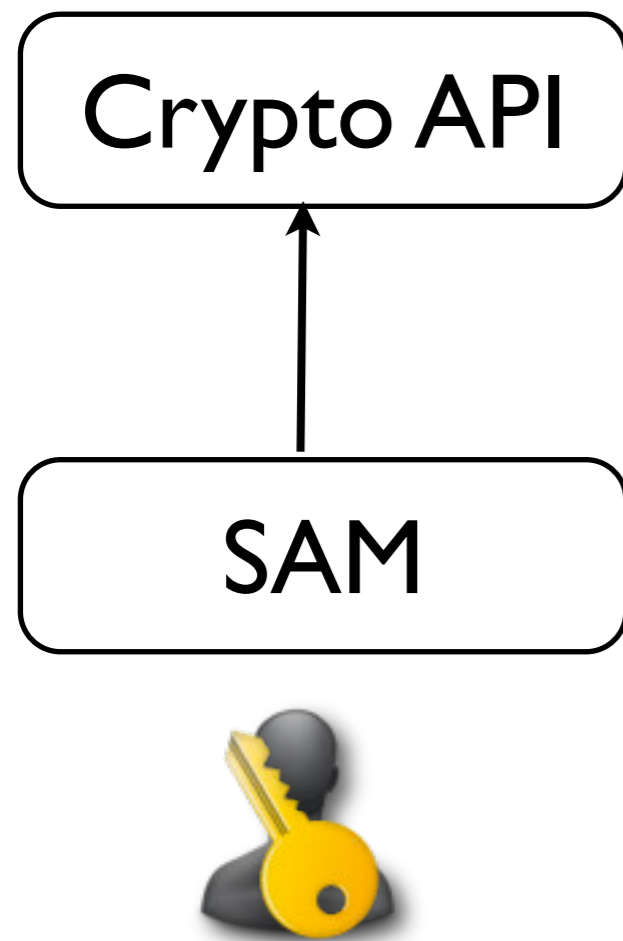
Why do we care about Windows crypto ?



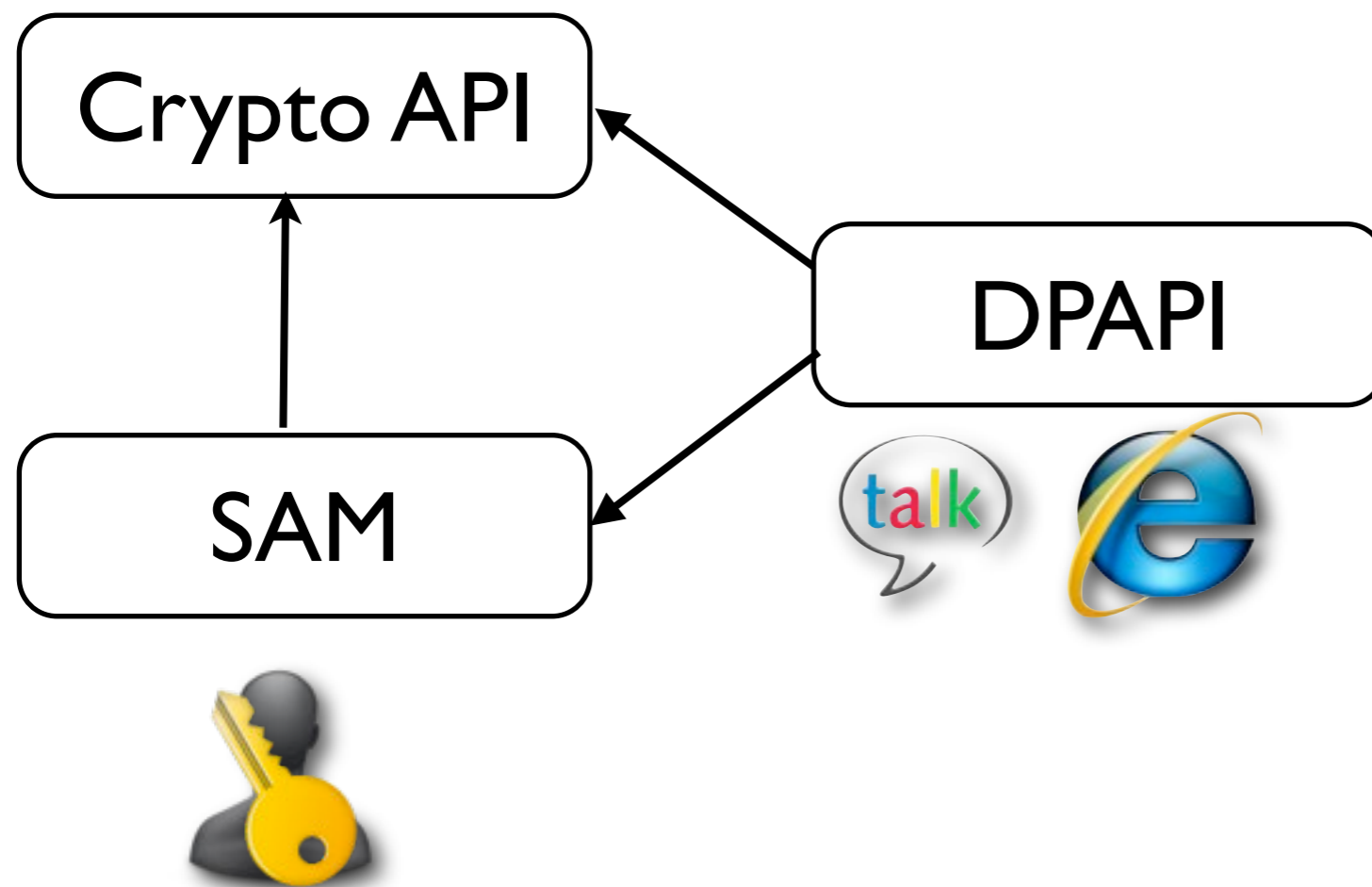
The Windows crypto eco-system

Crypto API

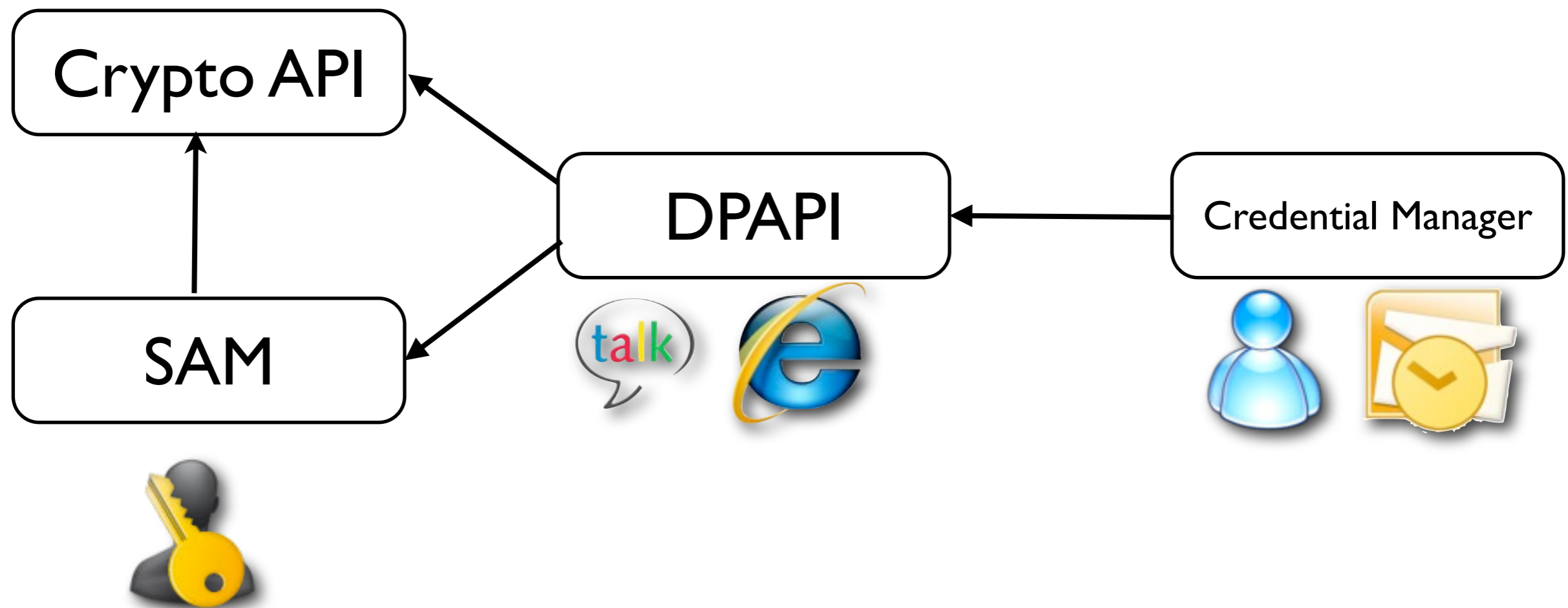
The Windows crypto eco-system



The Windows crypto eco-system



The Windows crypto eco-system

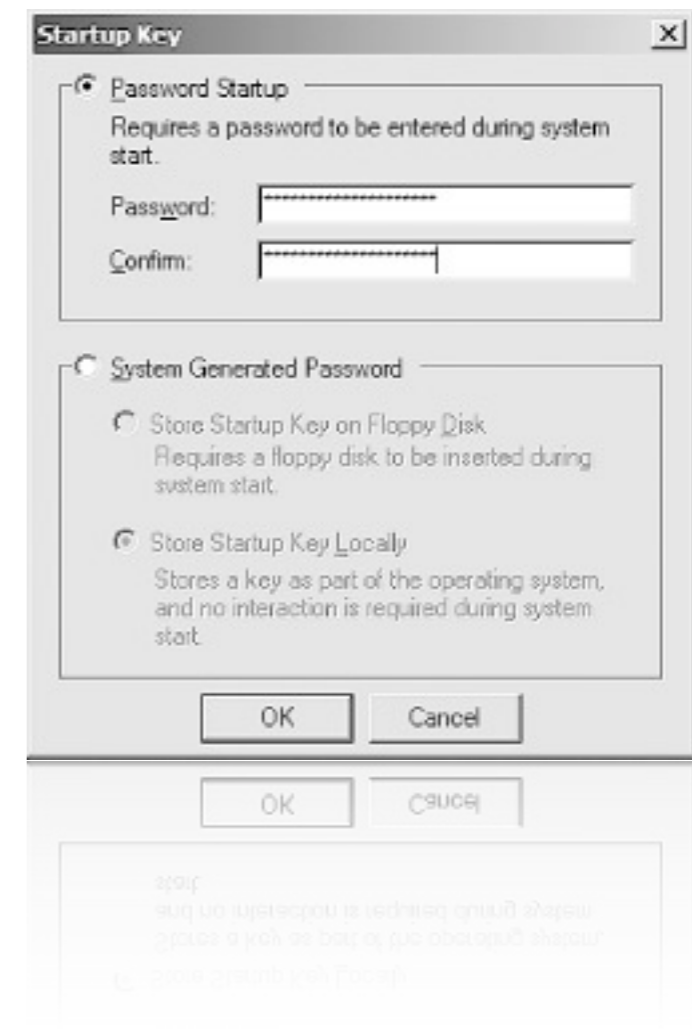


Windows Crypto API

- **Basic cryptographic blocks**
 - Cipher: 3DES, AES
 - Hash functions: SHA-1 SHA256, HMAC
 - PKI: public keys and certificates (X.509)

The Security Account Manager (SAM)

- Store Windows user credentials
- Located in the registry
- Encrypted with the SYSKEY
- Passwords are hashed



Windows Password Hashing functions

- Two hash functions used
 - LM hash function (NT, 2K, XP, VISTA) **weak**
 - NTLM (XP, Vista, 7)
- Passwords are **not salted**

LM hash weakness

- Use only upper-case
- Hash password in chunk of 7 characters

mypassword → LMHash(MYPASSW) + LMHash(ORD)

Password key-space: 69^7 (at most)

Rainbow Tables

- Pre-compute all the possible passwords
- Time-Memory trade-off
- Rainbow tables of **all** the LM hash are available

How OWADE Works

- Extract Usernames and password hashes
- LM hashes available ?
 - use John/Rainbow tables to get the pass in uppercase
 - use NTLM hashes to find the password cases
- Try to crack the NTLM using John/Rainbow table

Windows Password recovered

← → http://localhost:8080/owade/result_partition_1 ☆ ↻ 🇺🇸 css li

Quick Access
Passwords
Linkedin

Datas
Slot: 0
Offset: 63
Size: 78107967
Type: NTFS (0x07)

[Expand All](#) | [Contract All](#)

- WebAnalyze
- ProgramAnalyze
- GetUserPassword
 - DPAPI_SYSTEM: AQAANjSjMjGf9lsl4KEJbdSE7QpYKyJrsniDPcxe6s/pCj0ApjtsF5oc8=
 - Administrator
 - Guest
 - Ashee
 - id: 1003
 - name: Ashee
 - nthash: 31d6cfe0d16ae931b73c59d7e0c089c0
 - lmhash: aad3b435b51404eeaad3b435b51404ee
 - lmpass: empty
 - UpdatusUser
 - HelpAssistant
 - id: 1000
 - name: HelpAssistant
 - nthash: 6db41a7f826d75b655976315817291c
 - lmhash: 634299690515b074fdb81e98a2be98a
 - lmpass: Unknown
 - SUPPORT_388945a0
 - GetUserEnvironmentDetail
 - GetSoftwareEnvironmentDetail
 - GetSystemEnvironmentDetail
 - GetSoftwareDetail
 - GetUserConfigurationDetail
 - GetOSDetail
 - GetHardwareDetail
 - FilesStatistics





If the password is too strong we **can't recover** it

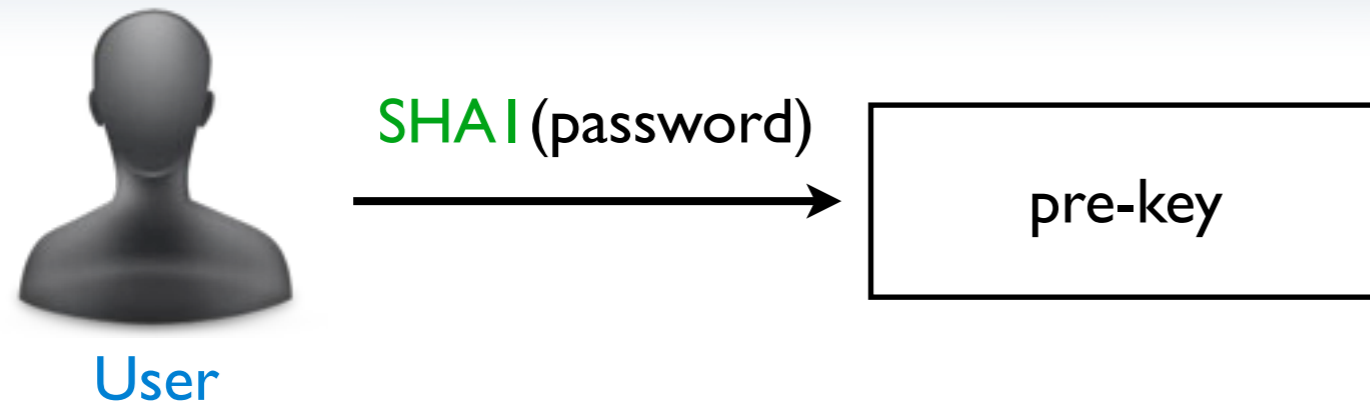


but we can **still decrypt** DPAPI secret (sometime)

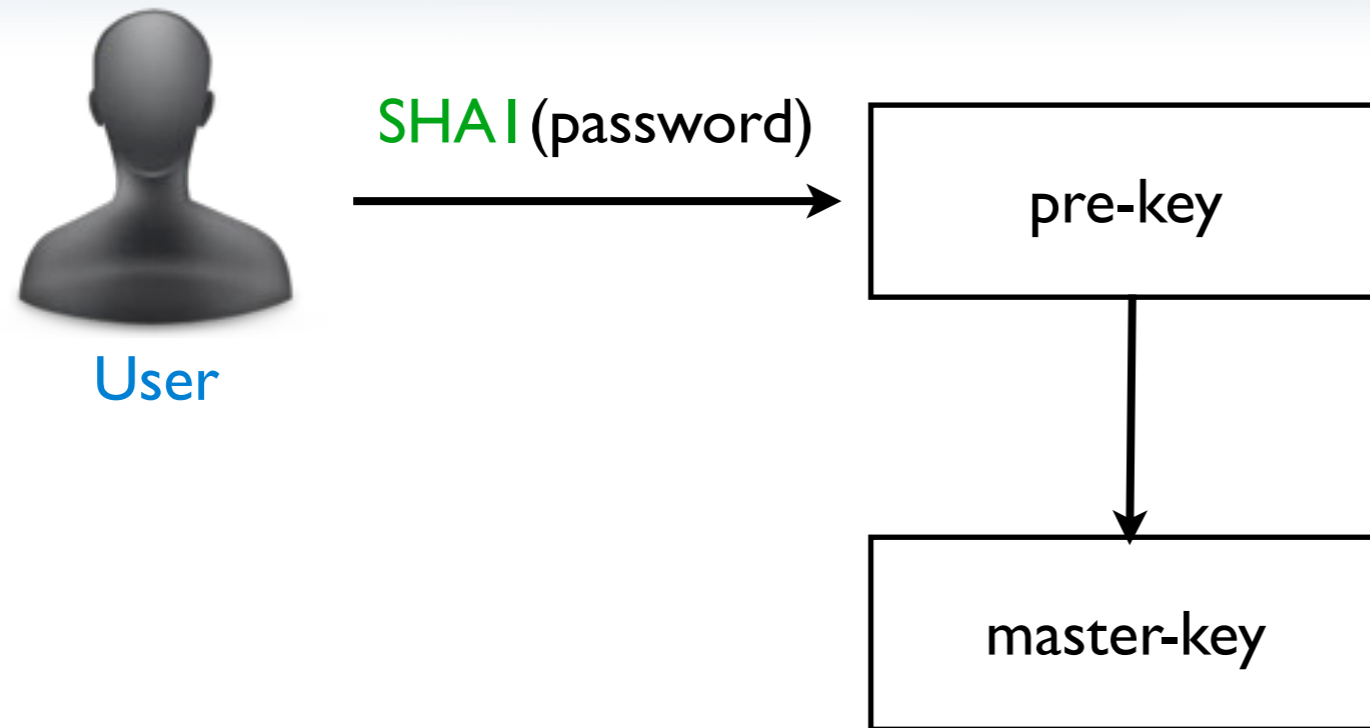
The Data Protection API

- Ensure that encrypted data can't be decrypted without knowing the user Windows password
- Blackbox crypto API for developers:
 - Encrypt data → DPAPI blob
 - Decrypt DPAPI blob → data
- Main point : tie the encryption to the user password

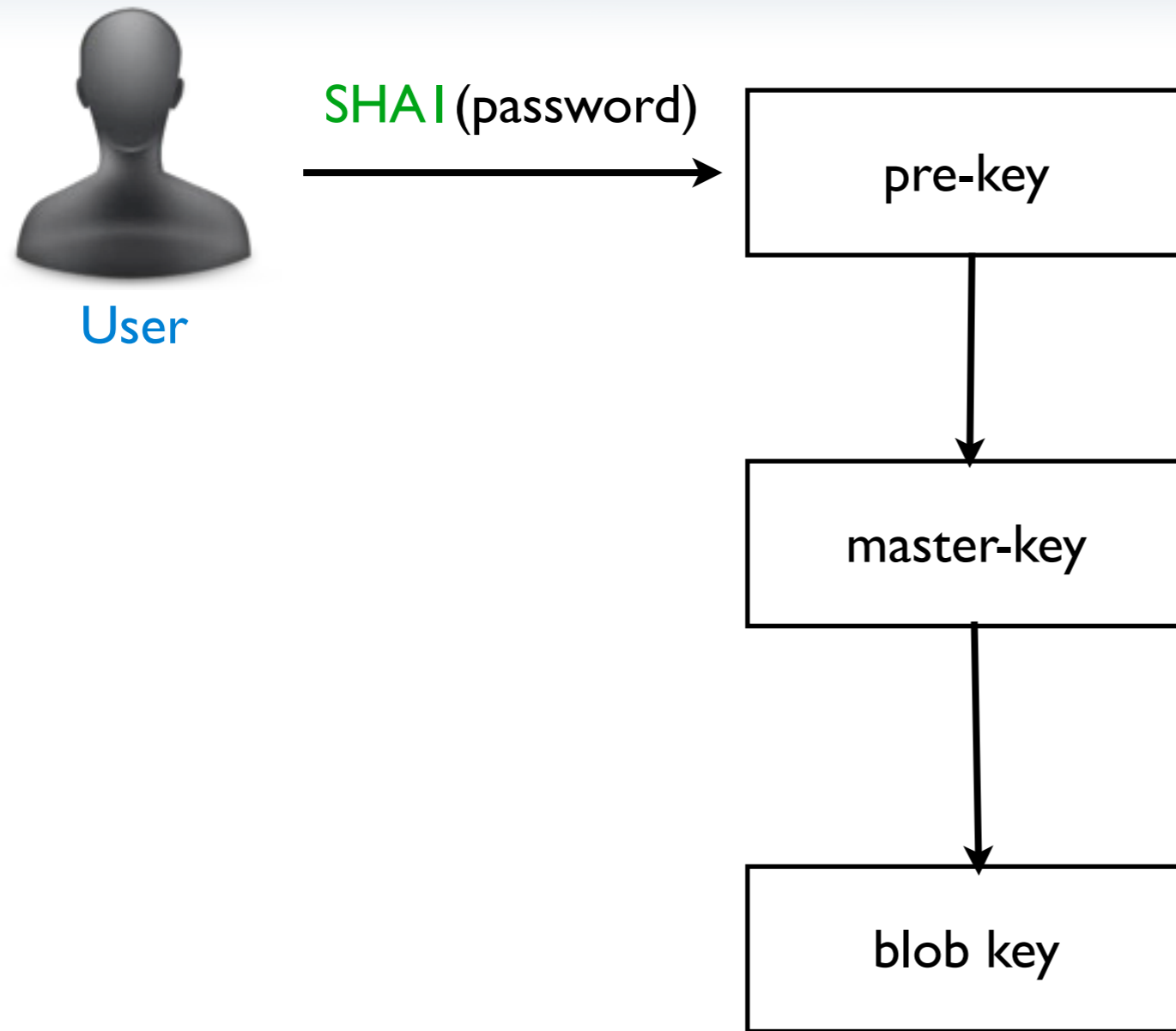
DPAPI derivation scheme



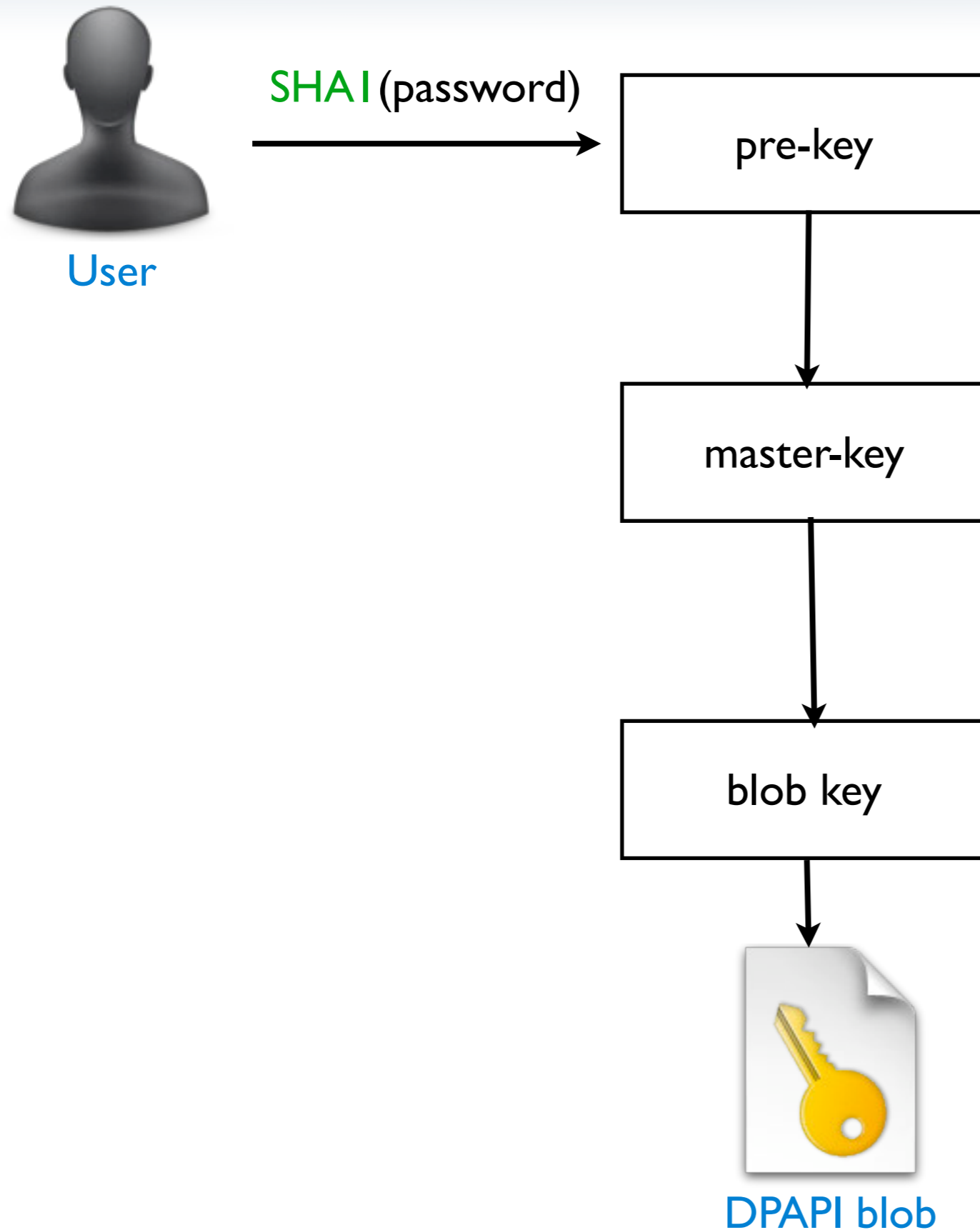
DPAPI derivation scheme



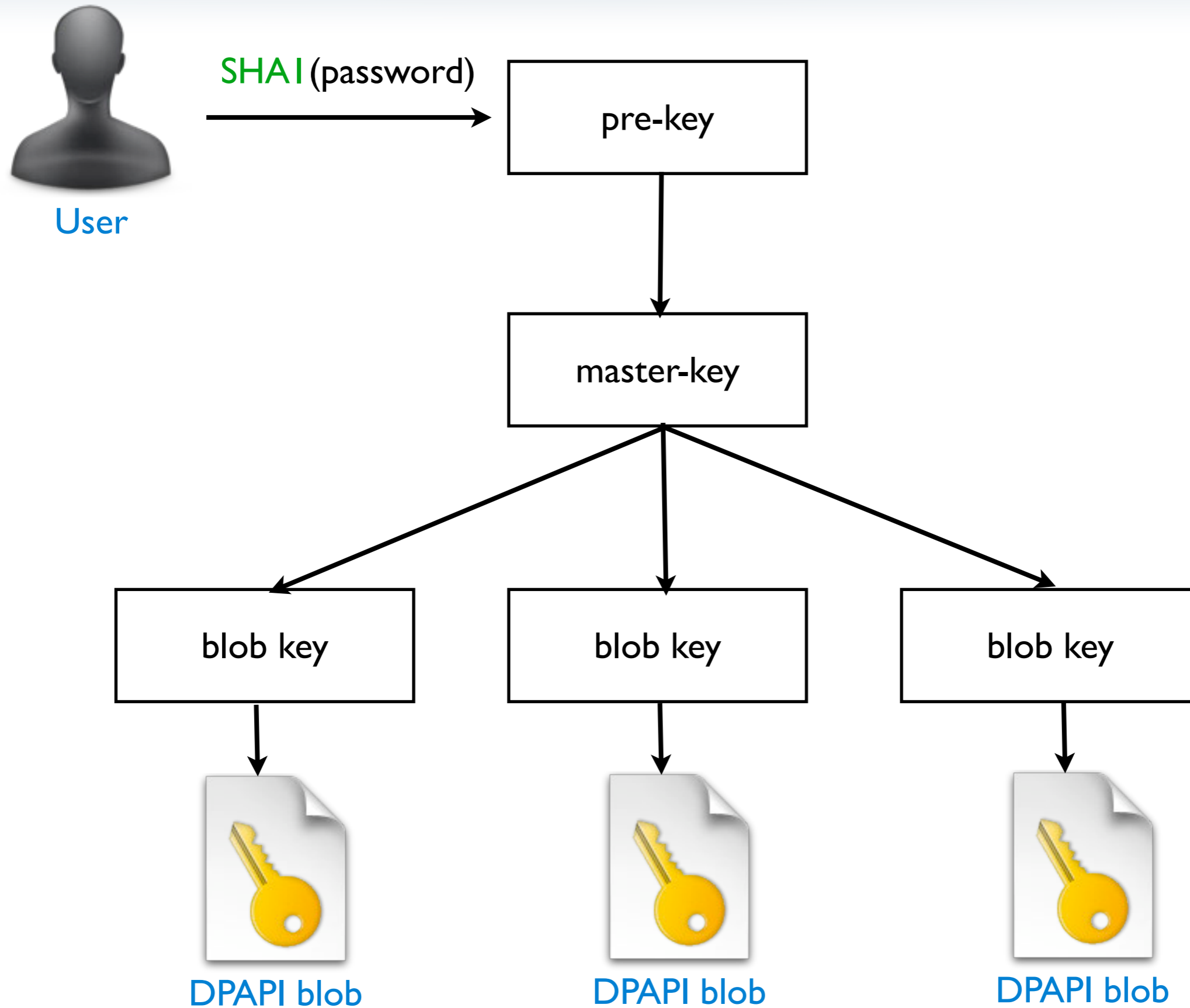
DPAPI derivation scheme



DPAPI derivation scheme



DPAPI derivation scheme



DPAPI Blob structure

```
struct wincrypt_datablob {
    DWORD    cbProviders,
    GUID     pbProviders[cbProviders],
    DWORD    cbMasterkeys,
    GUID     pbMasterkeys[cbMasterkeys],
    DWORD    dwFlags,
    DWORD    cbDescription,
    BYTE     pbDescription[cbDescription],
    ALG_ID   algCipher,
    DWORD    cbKey,
    DWORD    cbData,
    BYTE     pbData[cbData],
    DWORD    dwUnknown,
    ALG_ID   algHash,
    DWORD    dwHashSize,
    DWORD    cbSalt,
    BYTE     pbSalt[cbSalt],
    DWORD    cbCipher,
    BYTE     pbCipher[cbCipher],
    DWORD    cbCrc,
    BYTE     pbCrc[cbCrc]
} ;
```

DPAPI master-key structure

Header Structure

```
struct wincrypt_masterkey_masterkeybloc
{
    DWORD    dwRevision,
    BYTE     pbSalt[16],
    DWORD    dwRounds,
    ALG_ID   algMAC,
    ALG_ID   algCipher,
    BYTE     pbEncrypted[ ]
};
```

Footer Structure



DPAPI blob



DPAPI blob

Master-key GUID





DPAPI blob

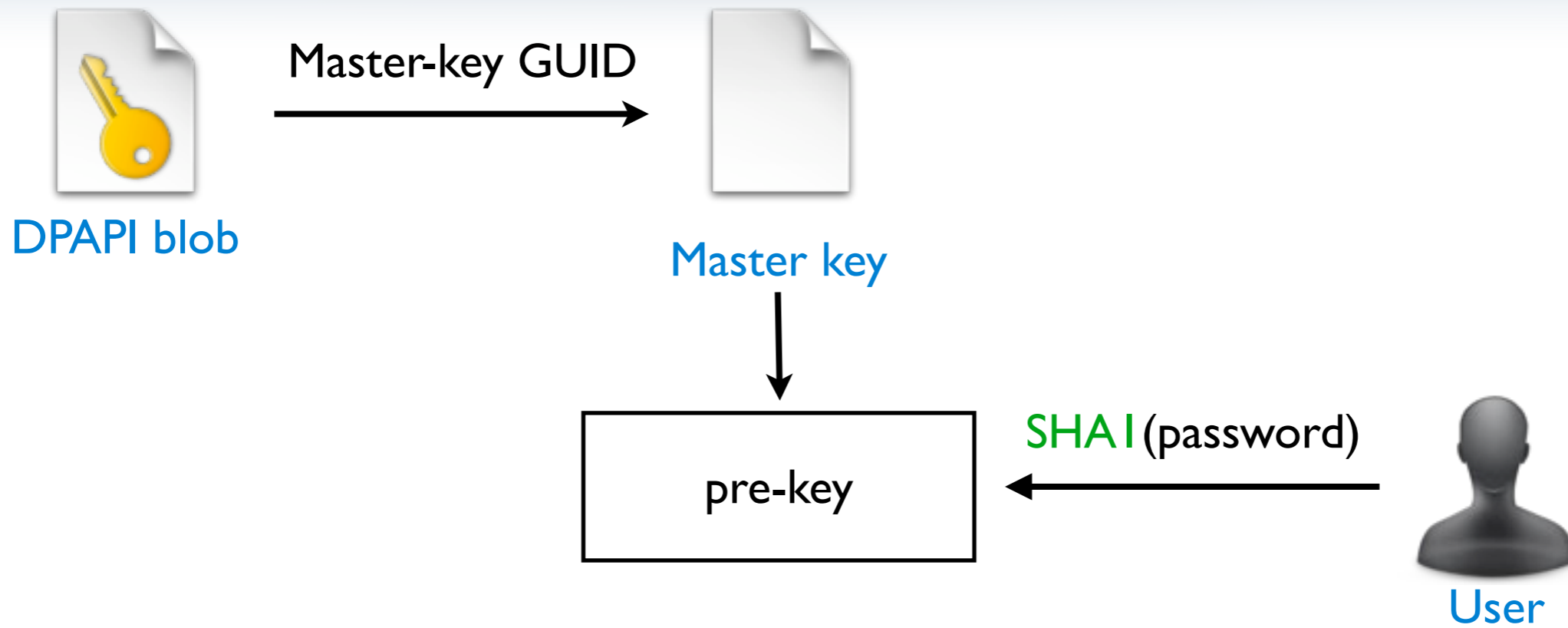
Master-key GUID

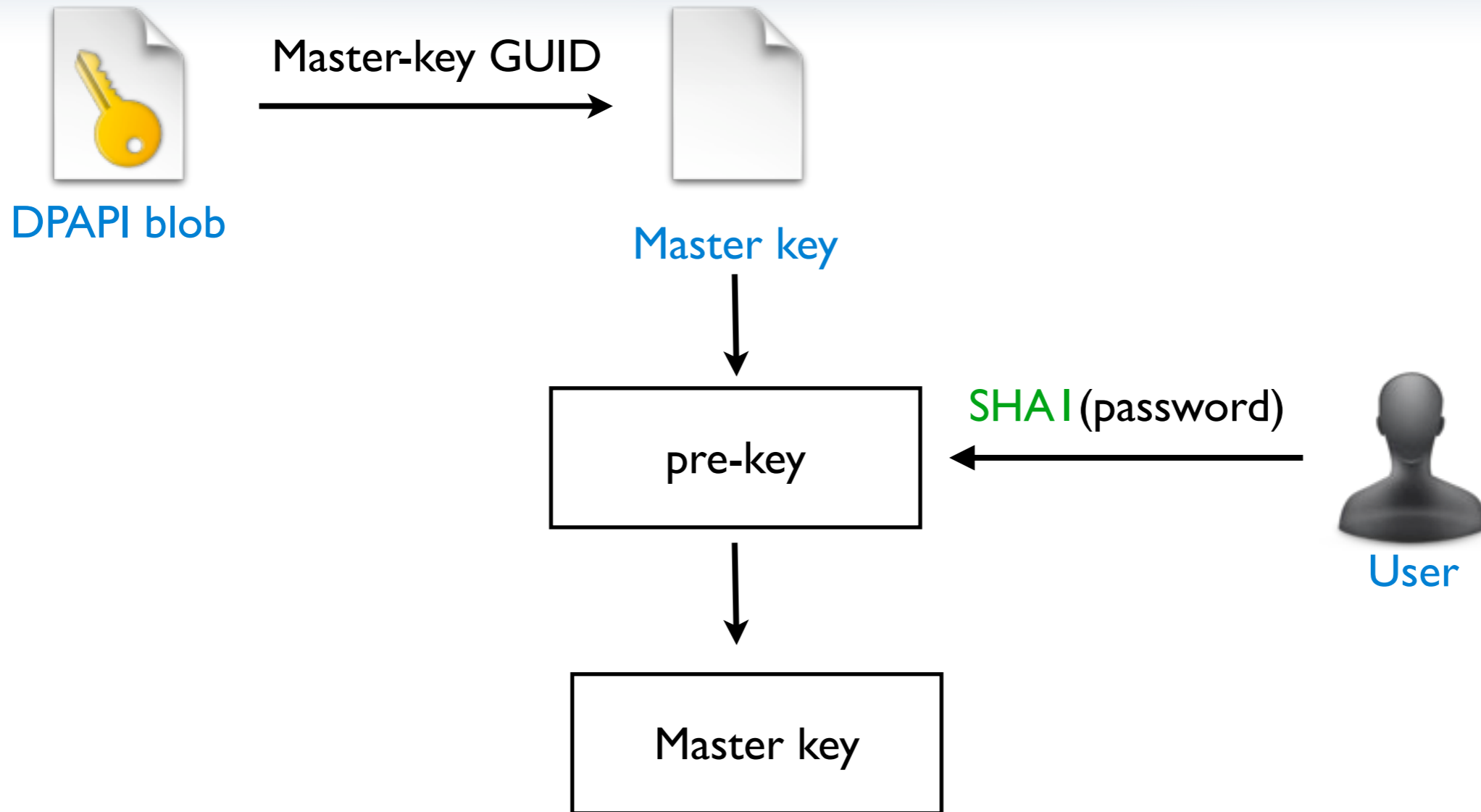


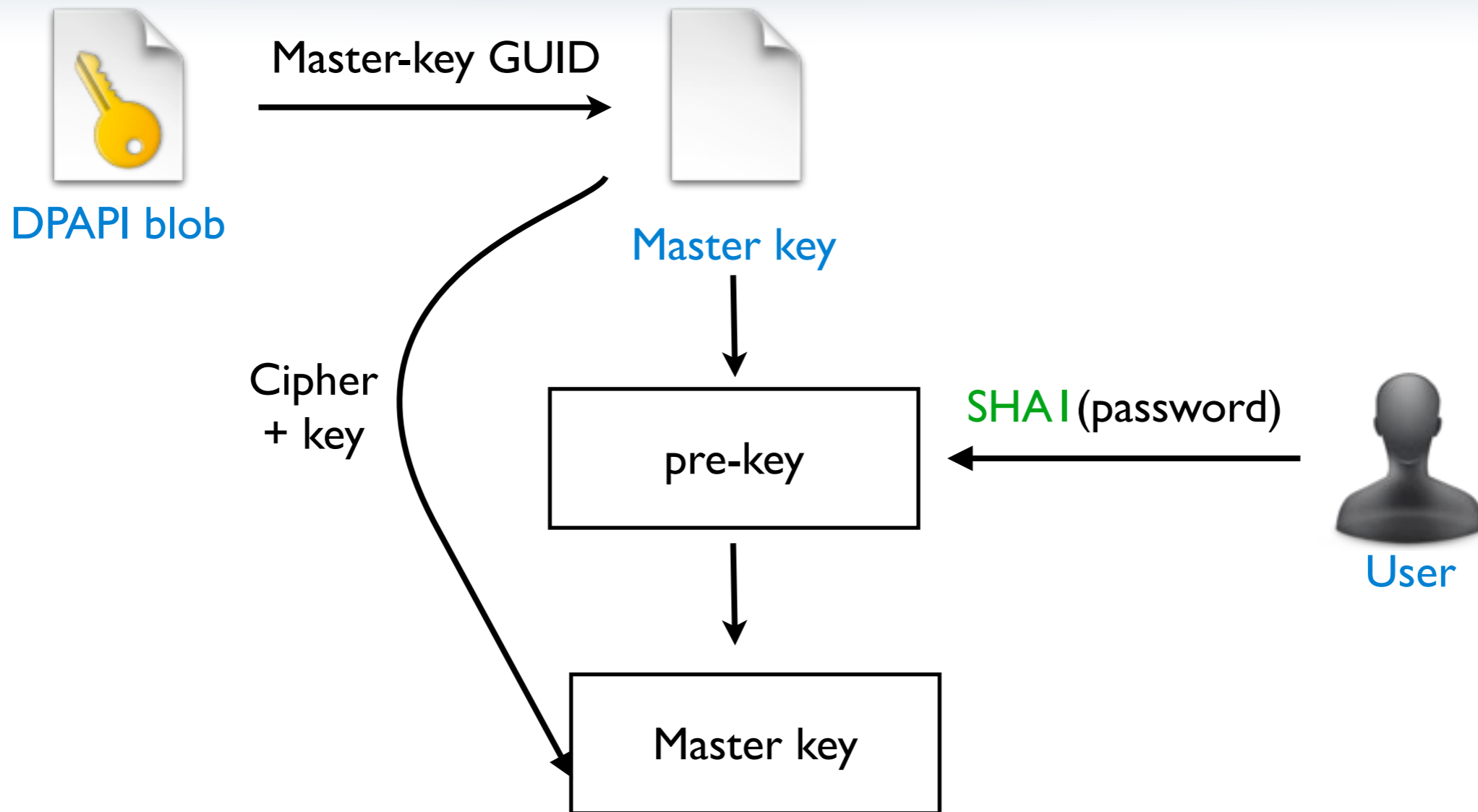
Master key

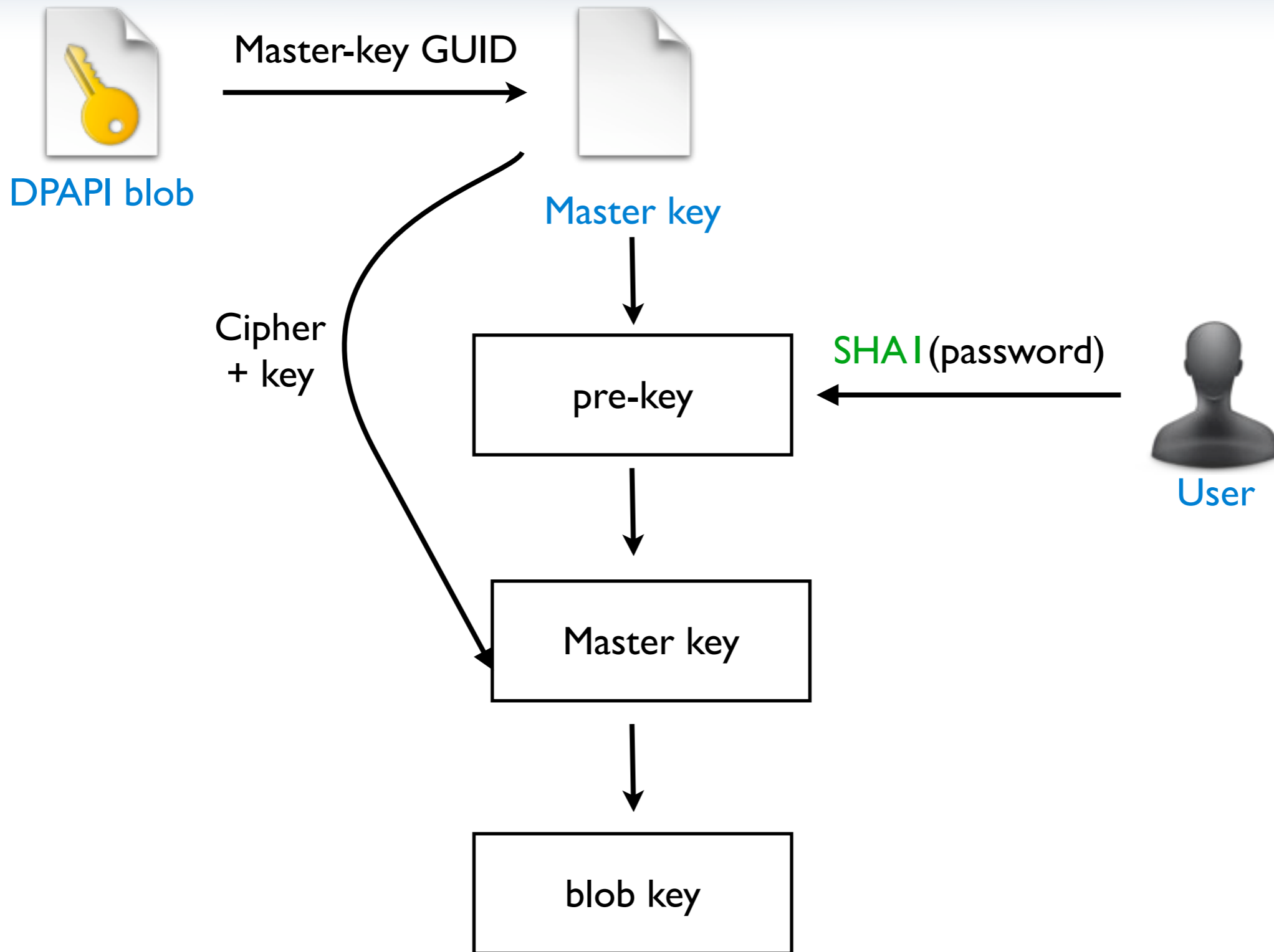


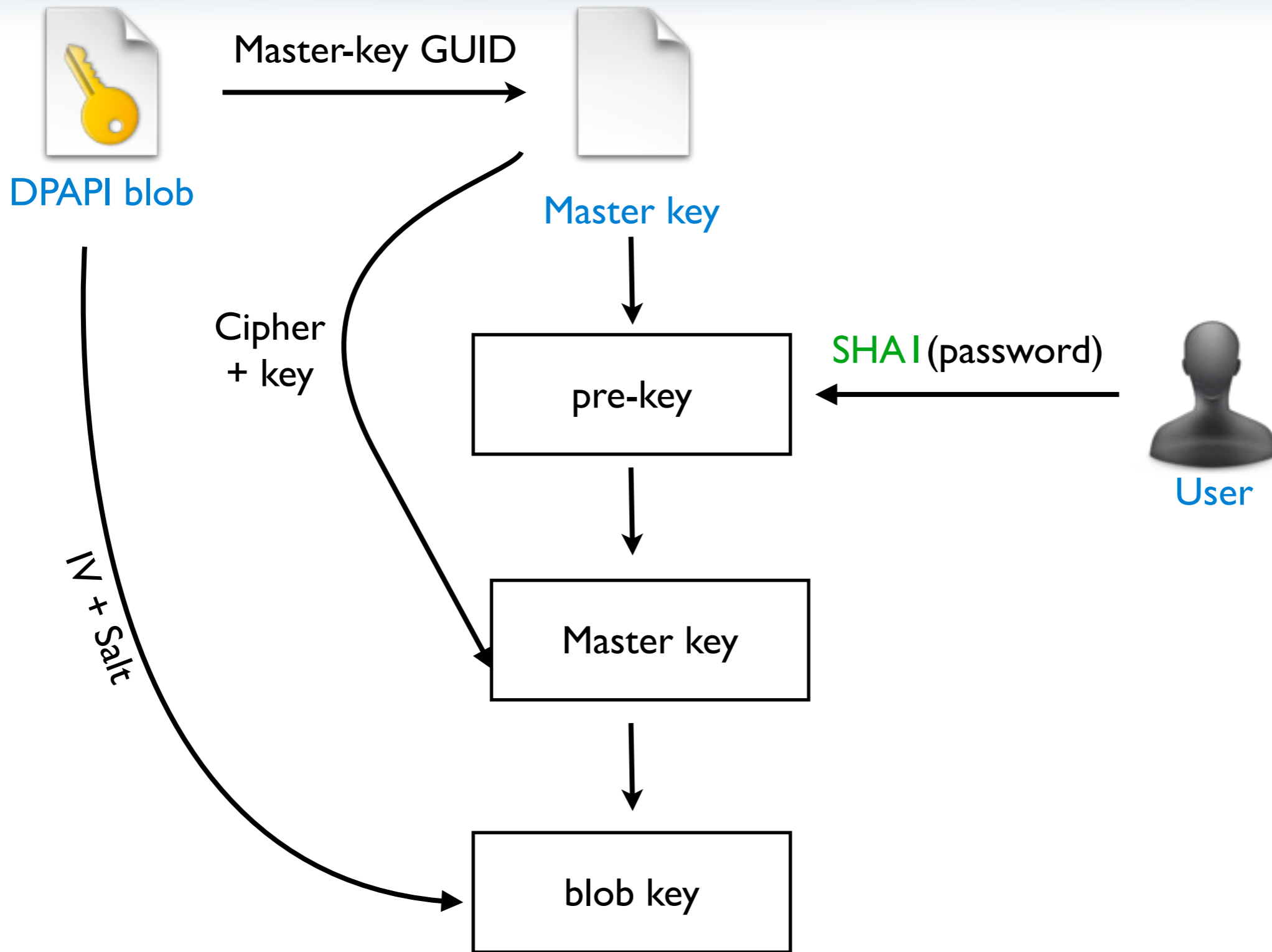
pre-key

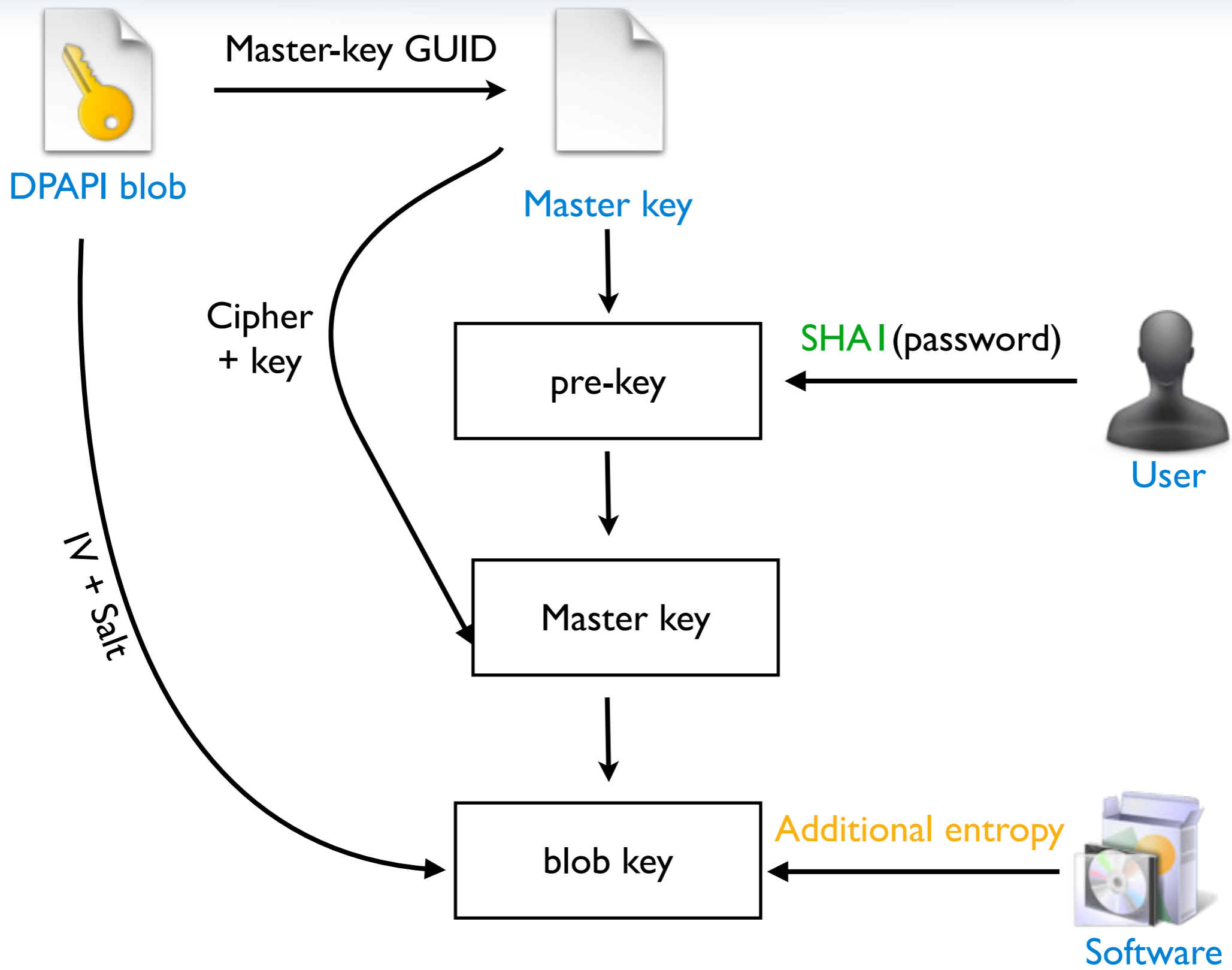












Bypassing the user password cracking

- If we can't crack the password we need its SHA1
- This **SHA1** is stored in the **hibernate file**
- OWADE uses Moonsoles to recover it



DPAPI additional entropy

- Software can supply an additional entropy
 - Act as a “key” (needed for decryption)
 - Force us to understand how it is generated for each software
 - Can be used to tie data to a specific machine (i.e Netbios name)

Credential Manager

- Built on top of DPAPI
- Handle transparently the encryption and storage of sensitive data
- Used by Windows, Live Messenger, Remote desktop...

Credstore type of credentials

Type of credential	Encryption	Example of application
Generic password	DPAPI + fixed string	Live messenger HTTP auth (IE)
Domain password	In clear	Netbios
Domain certificate	Hash of certificate	Certificate
Domain visible password	DPAPI + fixed string	Remote access .NET passport

WiFi data

Wifi data

- Info stored for each access point
 - Mac address (BSSID)
 - Key (encrypted)
 - Last time of access
- Wifi data are stored in
 - Registry (XP)
 - XML file and Registry (Vista/7)



Decrypting WiFi password

- Encrypted with DPAPI
- Access point shared among users
- Encrypted with the System account
- But the system account has no password...



What is my DPAPI key ???

Decrypting WiFi password

- Use a LSASecret as DPAPI key
- Array of credentials
 - HelpAssistant password in clear
 - DPAPI_SYSTEM
 - “Encrypted”



Where are you ?

- We've recovered access point **keys** but **where** are they ?



Where are you ?

- We've recovered access point **keys** but **where** are they ?



HTML5 Geo-location protocol

mozilla

Visit Mozilla.com

Location-Aware Browsing

Firefox can tell websites where you're located so you can find info that's more relevant and more useful. It's about making the Web smarter – and is done in a way that totally respects your privacy. [Give it a try!](#)



Frequently Asked Questions

- + What is Location-Aware Browsing?
- + How does it work?
- + How accurate are the locations?
- + What information is being sent, and to whom? How is my privacy protected?
- + Am I being tracked as I browse the web?
- + Am I being tracked as I browse the web?

HTML5 Geo-location protocol

Geolocation in Firefox - Mozilla Firefox

http://www.mozilla.com/en-US/firefox/geolocation/

Geolocation in Firefox

www.mozilla.com wants to know your location. [Learn More...](#) Share Location Don't Share Remember for this site

mozilla Visit Mozilla.com

Location-Aware Browsing

Firefox can tell you where you are. This information can be used to find information that is useful. It's about location-aware browsing. This is done in a way that respects your privacy. Give it a try.

Frequently Asked Questions

- + What is Location-Aware Browsing?
- + How does it work?
- + How accurate are the locations?

Map Satellite Hybrid

Asia North America Europe Africa South America Australia

Indian Ocean Atlantic Ocean Pacific Ocean

POWERED BY Google

Terms of Use

Where am I?

HTML5 Geo-location protocol

The screenshot shows a Firefox browser window with the address bar displaying `http://www.mozilla.com/en-US/firefox/geolocation/`. A notification bar at the top of the page reads "www.mozilla.com wants to know your location. [Learn More...](#)" and includes buttons for "Share Location", "Don't Share", and a checkbox for "Remember for this site". A yellow arrow points to the "Share Location" button. The main content area features the Mozilla logo and the heading "Location-Aware Browsing". Below this, a map interface is displayed, which includes a "Where am I?" button, a "Map" button, and "Satellite" and "Hybrid" map style options. The map shows a world map with labels for continents and oceans. A cartoon character is visible on the right side of the page.

Behind the curtain

PCWorld News Reviews How-To Downloads

Magazine
Subscribe & Get a Bonus CD
Customer Service

THE NEW M11x : The Most Powerful 11-inch Laptop In The Universe

PCWorld » Blogs » Today @ PCWorld

1 digg ShareThis

Google Wi-Fi Data Collection Angers European Officials

Brennon Slattery, PC World May 17, 2010 7:08 am

European officials are still miffed over [Google's "accidental" Wi-Fi data collection](#) and seek an in-depth investigation that may lead to harsh penalties for the search engine giant.

[It was revealed](#) that Google's [Street View](#) cars were collecting more than images and coordinates for its sophisticated GPS site. As much as 600GB of data from Wi-Fi networks -- in more than 30 countries -- [has been snagged in Google's fishnet](#).

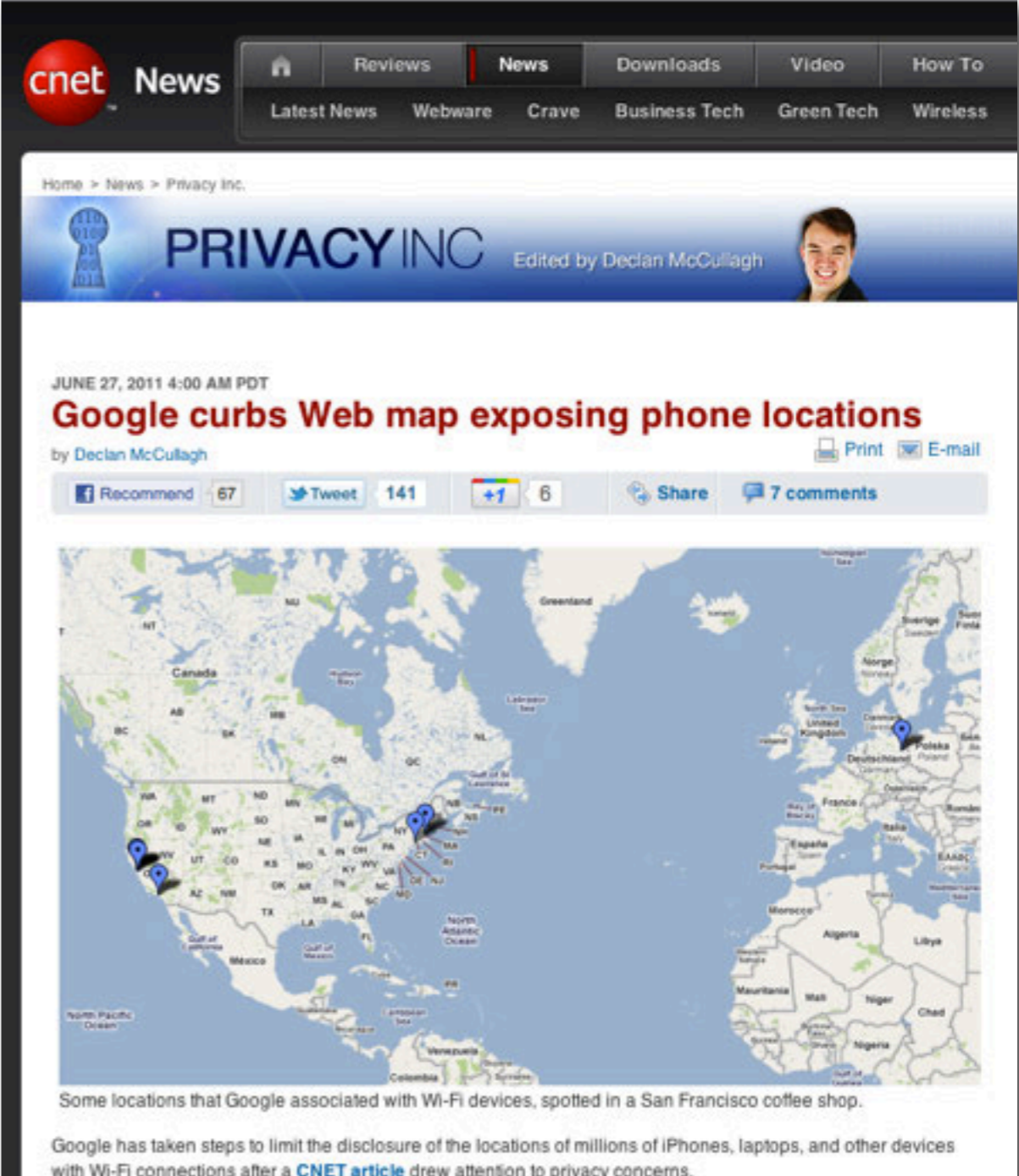


Artwork: Chip Taylor



Nothing is ever easy

- Google started to restrict queries in June
- So we started to look for other API



The screenshot shows a CNET News article page. At the top, there's a navigation bar with 'cnet News' and various menu items like 'Reviews', 'News', 'Downloads', 'Video', and 'How To'. Below that, a sub-navigation bar lists 'Latest News', 'Webware', 'Crave', 'Business Tech', 'Green Tech', and 'Wireless'. The article's breadcrumb trail is 'Home > News > Privacy Inc.'. The main header features the 'PRIVACY INC' logo and a photo of the author, Declan McCullagh, with the text 'Edited by Declan McCullagh'. The article title is 'Google curbs Web map exposing phone locations' in red, dated 'JUNE 27, 2011 4:00 AM PDT'. Below the title are social media sharing options: 'Recommend 67', 'Tweet 141', '+1 6', 'Share', and '7 comments'. The main content area shows a map of the United States with several blue location pins. Below the map, the text reads: 'Some locations that Google associated with Wi-Fi devices, spotted in a San Francisco coffee shop.' At the bottom, a paragraph states: 'Google has taken steps to limit the disclosure of the locations of millions of iPhones, laptops, and other devices with Wi-Fi connections after a [CNET article](#) drew attention to privacy concerns.'

Entering Microsoft

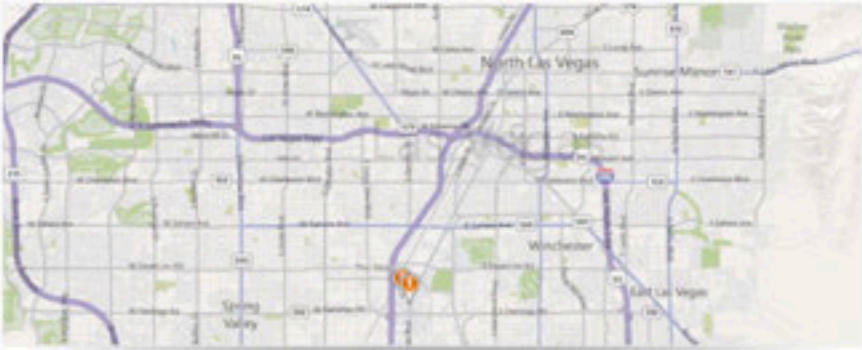
- Live service
- “Documented” in the Windows mobile MSDN
- After sniffing the traffic:
 - Use a big SOAP request
 - Does not check any ID fields
 - Allows to supply one MAC


```
<GetLocationUsingFingerprint xmlns="http://inference.location.live.com">
  <RequestHeader>
    <Timestamp>2011-02-15T16:22:47.0000968-05:00
    </Timestamp>
    <ApplicationId>e1e71f6b-2149-45f3-b298-a20XXXXX5017
    </ApplicationId>
    <TrackingId>21BF9AD6-CFD3-46B2-B042-EE90XXXXXX
    </TrackingId>
    <DeviceProfile ClientGuid="0fc571be-4622-4ce0-b04e-XXXXXXeb1a222" Platform="Windows7" DeviceType="PC" OSVersion="7600.16695.amd64fre.win7_gdr.101026-1503" LFVersion="9.0.8080.16413" ExtendedDeviceInfo="" />
    <Authorization />
  </RequestHeader>
  <BeaconFingerprint>
  <Detections>
    <Wifi7 Bssid="00:BA:DC:0F:FE:00" rssi="-25" />
  </Detections>
  </BeaconFingerprint>
</GetLocationUsingFingerprint>
```

Blog post and demo released !


From Information to Intelligence Home
Dealing with information in the digital age


Using the Microsoft Geolocation API to retrace where a Windows laptop has been
July 29, 2011 | Privacy 4 Comments and 93 Reactions



About the author
 Elie Bursztein
I am a security researcher at Stanford University. This blog is about security, and more broadly about web technologies.

Search ..

Subscribe and follow us


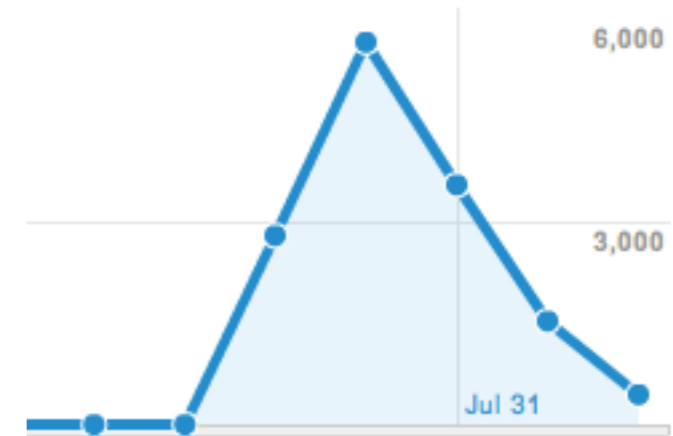
Latest Security Report
 Report from the security front-lines July 18 th 24th July 26, 2011

EDIT (Tuesday 2nd August) Microsoft Statement is available from [here](#)






EDIT (Sunday 31th July) The flaw is fixed: I had a phone call with some people from Microsoft yesterday (yes on a Saturday) and they told me they fixed the problem. I will update this post with their response as soon as it is out. The demo code does not work anymore.

In our [upcoming BlackHat talk](#), we will show you how the WiFi data stored by Windows can be used to geolocate where your computer has been. While the ability to retrace where a computer has been (and when) certainly carries privacy implications, in this post I want to focus on how we uncovered this data, and the unexpected difficulties we encountered while developing this technique.

Like 27 **Share 15** **2** **3 points** **12** **Tweet 100**



13,188 people visited this site

-  **13,963 Visits**
-  **13,188 Unique Visitors**
-  **51,805 Pageviews**
-  **3.71 Pages/Visit**
-  **00:02:04 Avg. Time on Site**
-  **22.94% Bounce Rate**
-  **94.13% % New Visits**

Just fixed

- Fixed last weekend
- No longer return location for a single address



Microsoft
Microsoft Privacy & Safety
Microsoft's Approach to Helping Protect Privacy and Safety

TechNet Blogs > Microsoft Privacy & Safety > Microsoft Makes Change to Geographic Location Positioning Service

Microsoft Makes Change to Geographic Location Positioning Service

 Microsoft Privacy Team 1 Aug 2011 11:58 AM |  0 RATE THIS


Updated 9:14 A.M. 8/2/2011

Microsoft released a change to its geographic location positioning service on July 30, 2011, which addresses an issue highlighted in Elie Bursztein's [blog](#) on July 29, 2011. This change adds improved filtering to validate each request so that the service will no longer return an inferred position when a single Media Access Control address is submitted. Microsoft is keenly aware of the sensitivity around all privacy issues, especially those surrounding geolocation.

Microsoft's privacy and security team has been in contact with Elie and we will continue the ongoing dialog with experts in the privacy field to improve our service offerings. We thank Elie, Matthieu Martin from Stanford University, Jean Michael Picod and Ivan Fontarensky from Cassidian for working with us on this issue.

Microsoft's commitment to privacy means that not only will we seek to build privacy into products, but we'll also engage with key stakeholders in government, industry, academia and public interest groups to develop more effective privacy and data protection measures. We will continue to update our service with improvements that benefit the consumer in both positioning accuracy as well as individual privacy.

Reid Kuhn is a Partner Group Program Manager on the Windows Phone engineering team at Microsoft
 Privacy

Just fixed

- Fixed last weekend
- No longer return location for a single address



Microsoft
Microsoft Privacy & Safety
Microsoft's Approach to Helping Protect Privacy and Safety

TechNet Blogs > Microsoft Privacy & Safety > Microsoft Makes Change to Geographic Location Positioning Service

Microsoft Makes Change to Geographic Location Positioning Service

Microsoft Privacy Team 1 Aug 2011 11:58 AM 0 RATE THIS ★★★★★

Updated 9:14 A.M. 8/2/2011

Microsoft released a change to its geographic location positioning service on July 30, 2011, which addresses an issue highlighted in Elie Bursztein's [blog](#) on July 29, 2011. This change adds improved filtering to validate each request so that the service will no longer return an inferred position when a single Media Access Control address is submitted. Microsoft is keenly aware of the sensitivity around all privacy issues, especially those surrounding geolocation.

Microsoft's privacy and security team has been in contact with Elie and we will continue the ongoing dialog with experts in the privacy field to improve our service offerings. We thank Elie, Matthieu Martin from Stanford University, Jean Michael Picod and Ivan Fontarensky from Cassidian for working with us on this issue.

Microsoft's commitment to privacy means that not only will we seek to build privacy into products, but we'll also engage with key stakeholders in government, industry, academia and public interest groups to develop more effective privacy and data protection measures. We will continue to update our service with improvements that benefit the consumer in both positioning accuracy as well as individual privacy.

Reid Kuhn is a Partner Group Program Manager on the Windows Phone engineering team at Microsoft
Privacy

There is a Patch for that!

Geo-location API restrictions

The Google logo, featuring the word "Google" in its characteristic multi-colored font (blue, red, yellow, blue, green, red) with a trademark symbol.

Requires 2 MAC
close from each other

The Skyhook Wireless logo, featuring a blue swoosh above the word "SKYHOOK" in a bold, serif font, with "WIRELESS" in a smaller, spaced-out, sans-serif font below it.

The MAC and IP location
need to be “close”

The Microsoft logo, featuring the word "Microsoft" in a bold, italicized, sans-serif font with a registered trademark symbol.

Requires multiples
MAC addresses

see <http://elie.im/blog/> for more information

WiFi Information Extracted By OWDE

http://localhost:8080/owade/result_partition_1

- Default User
- NetworkService
- GetXPWifiNetworks
 - wifi1
 - authentication: Open
 - last: 1311386932
 - ssid: SecLab-N 2.4Ghz
 - bssid: 98:fc:11:6f:99:1e
 - latitude: 0
 - hexkey:
 - longitude: 0
 - nettype: 802.11b/g
 - channel: 6
 - mode: Infrastructure
 - wifi2
 - authentication: WPA-PSK
 - last: 1311380261
 - ssid: DoNotConnect
 - bssid: 00:24:a5:42:d0:25
 - latitude: 0
 - hexkey: 25eef130c6a61f6106d337f7e6ec66aa9041eb1527f01850c635fcd02fe662d
 - longitude: 0
 - nettype: 802.11b/g
 - channel: 7
 - mode: Infrastructure
 - wifi3
 - authentication: Open
 - last: 1311380294
 - ssid: CS.Stanford.EDU
 - bssid: 00:18:0a:30:03:62
 - latitude: 0
 - hexkey:
 - longitude: 0
 - nettype: 802.11b/g
 - channel: 1
 - mode: Infrastructure
 - wifi4
- LocalService
- Ashee



47

Browsers

Firefox > 3.4

- Passwords
 - Location: **signons.sqlite**
 - Encryption: **3DES + Master password**
- History
 - URLs: **places.sqlite**
 - Forms fields: **formhistory.sqlite**



Firefox

Take back the web

Decrypting Firefox password

Decrypting Firefox password



User

pass



Decrypting Firefox password



User

pass

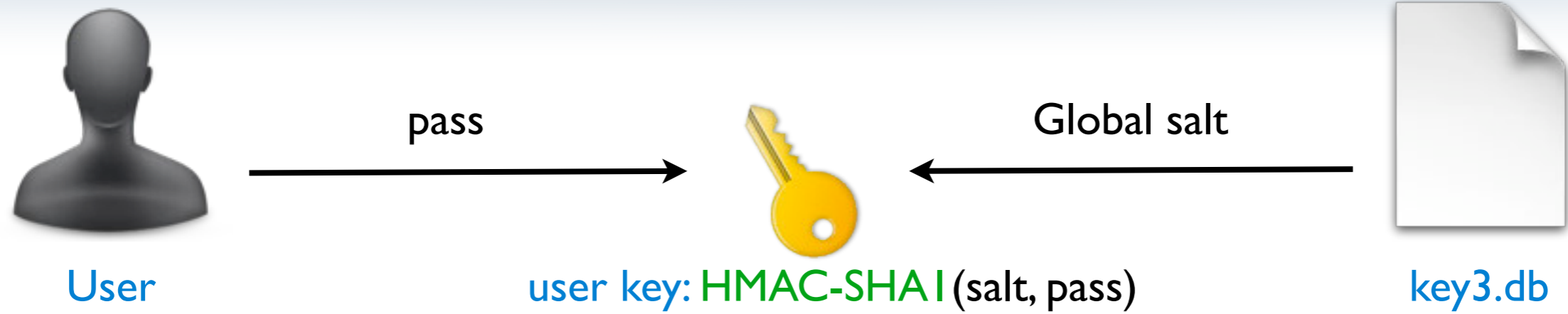


Global salt

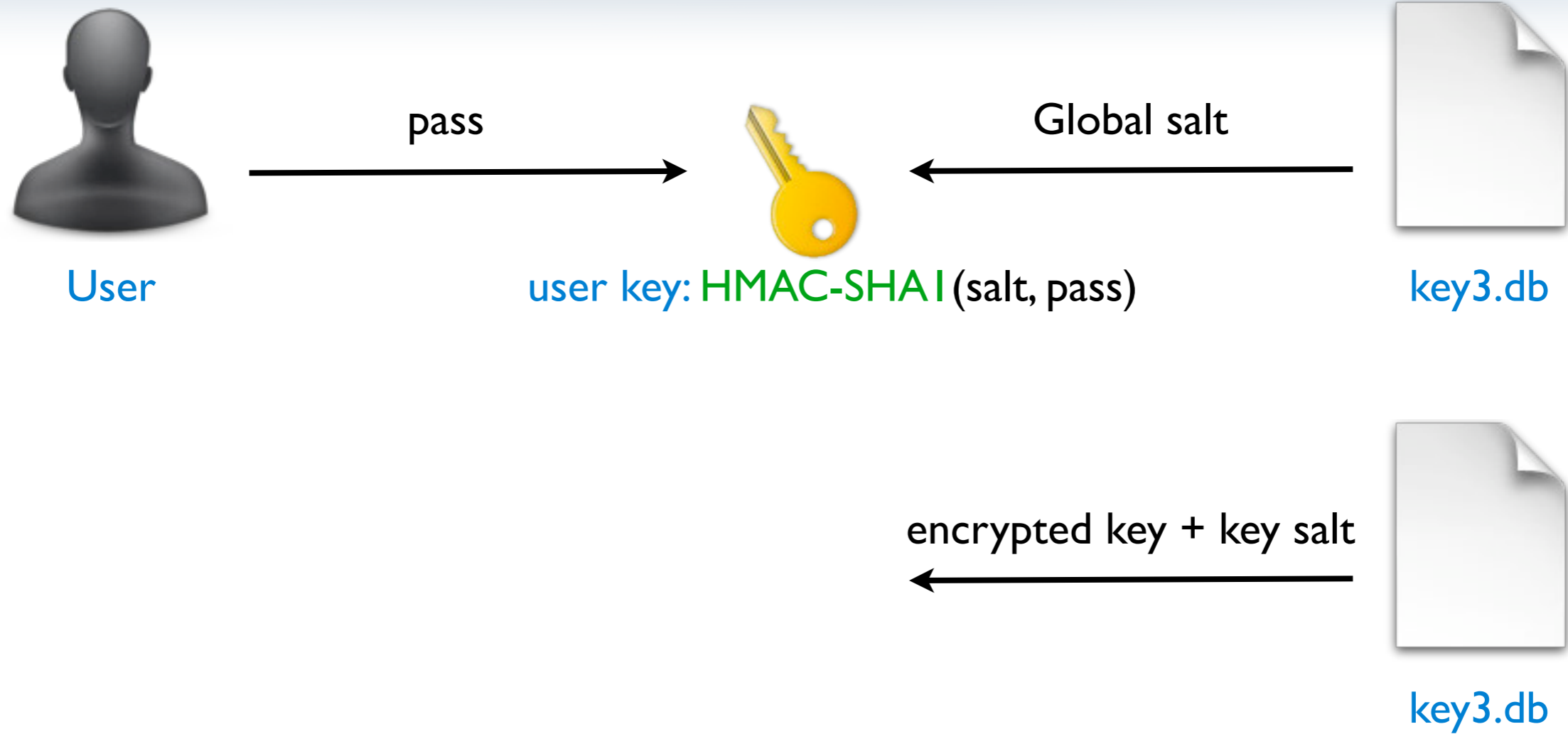


key3.db

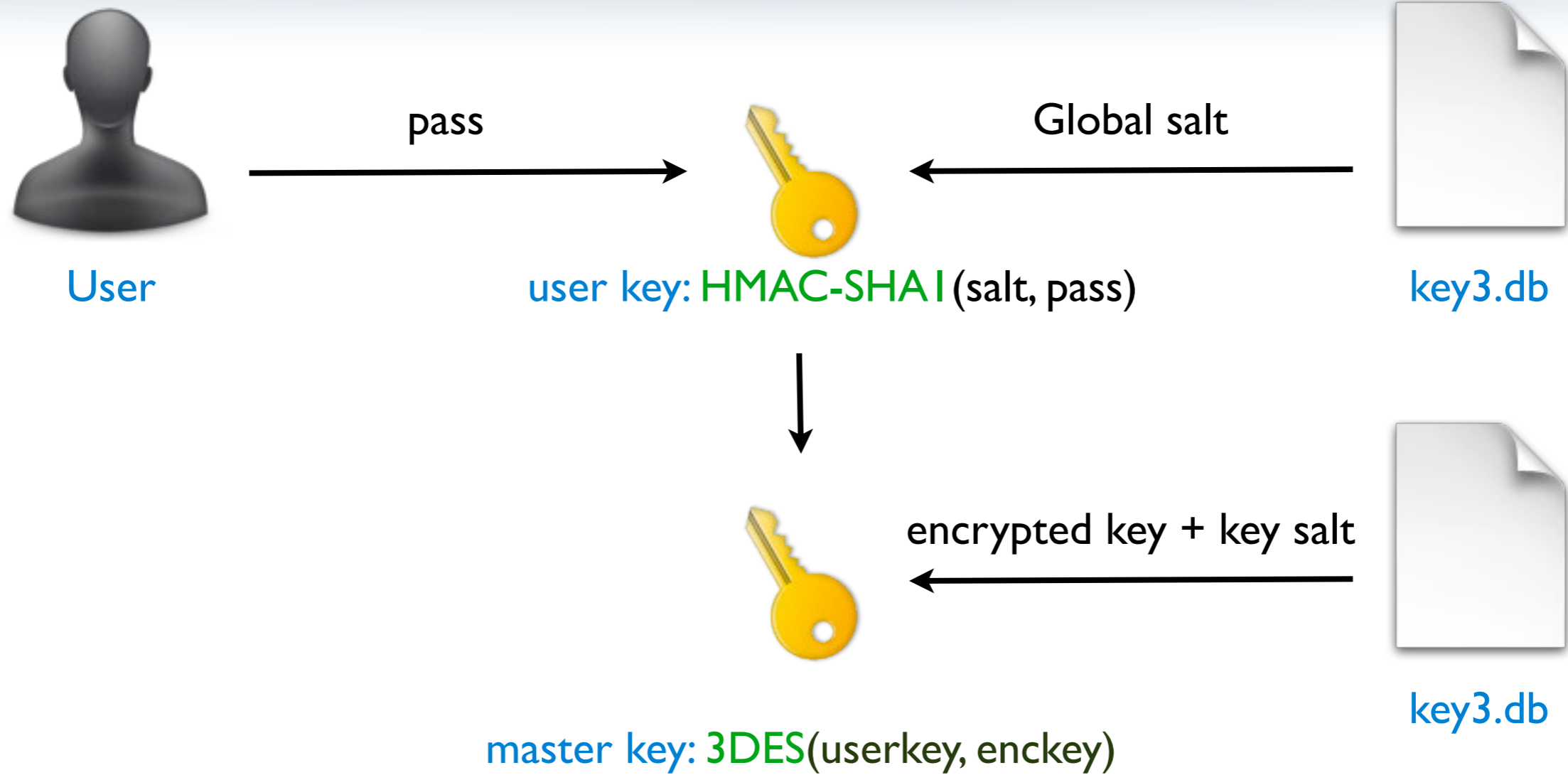
Decrypting Firefox password



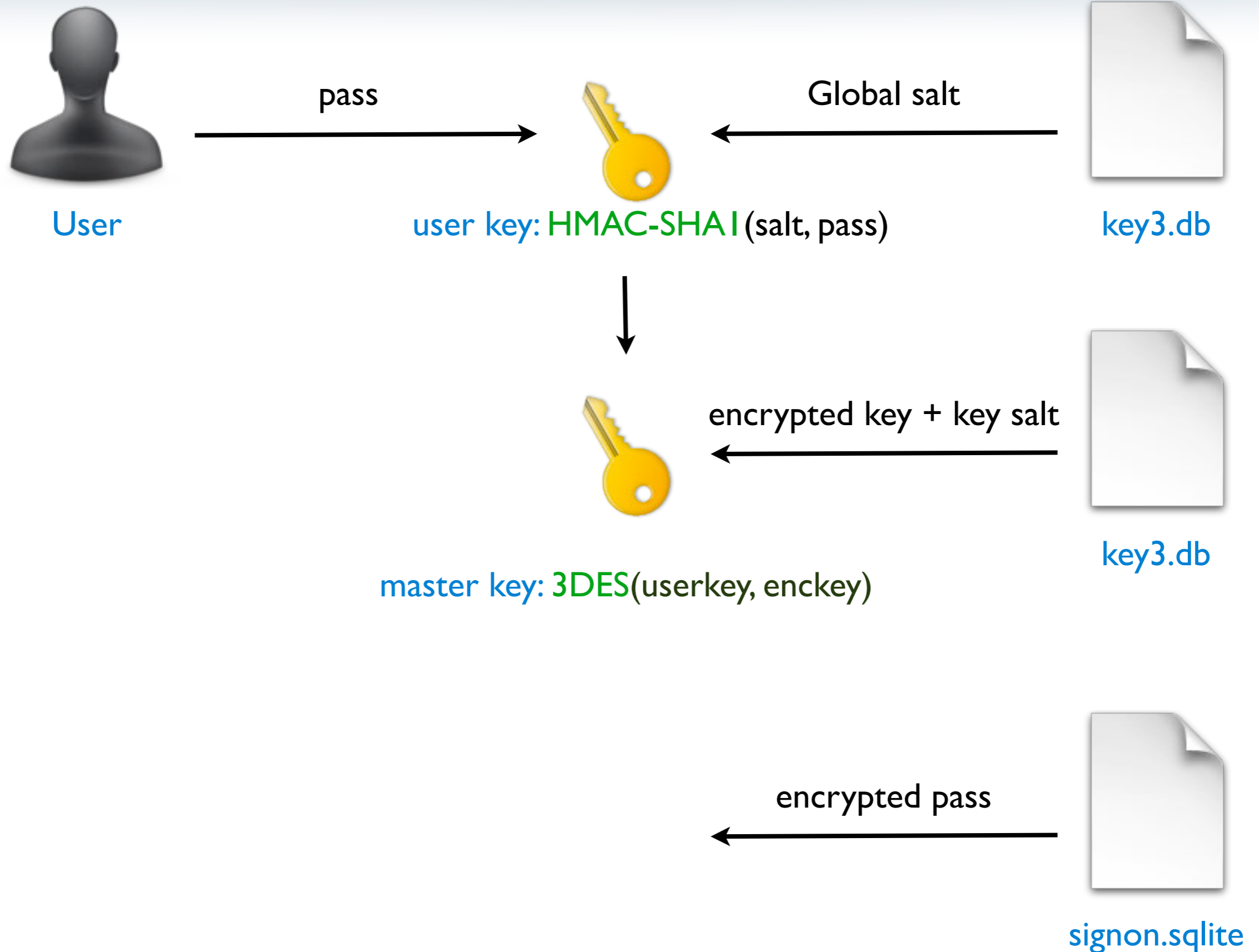
Decrypting Firefox password



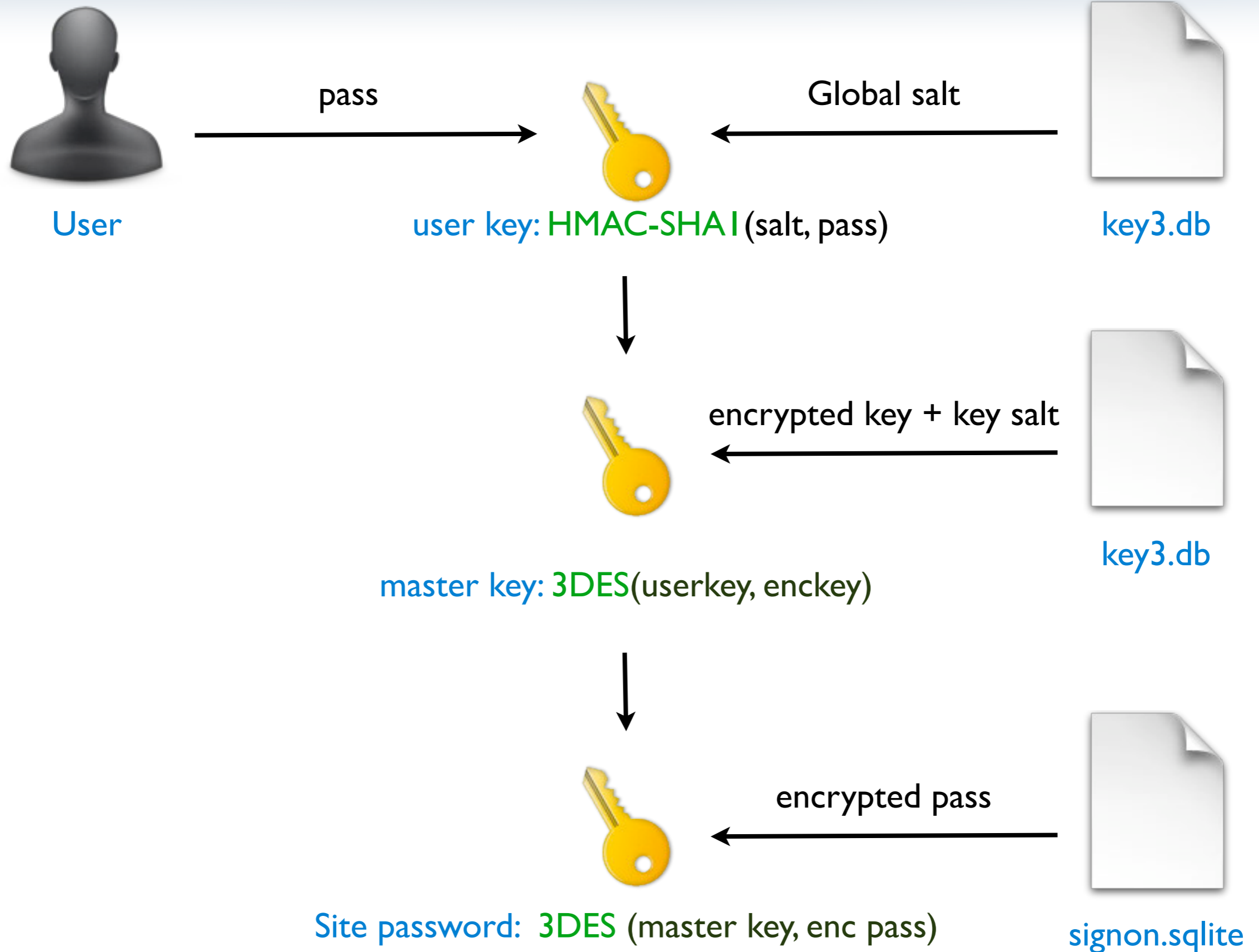
Decrypting Firefox password



Decrypting Firefox password



Decrypting Firefox password



Shopping at Amazon ?

The screenshot shows the Amazon.com homepage in a Firefox browser window. The browser's address bar displays "Amazon.com: Online Shopping for El...". The Amazon logo is in the top left, and the navigation bar includes links for "Sign in", "Start here", "Today's Deals", "Gifts & Wish Lists", and "Gift Cards". A search bar is prominently featured with a "GO" button. On the left, a vertical menu lists various departments such as "Unlimited Instant Videos", "MP3s & Cloud Player", "Amazon Cloud Drive", "Kindle", "Appstore for Android", "Digital Games & Software", "Audible Audiobooks", "Books", "Movies, Music & Games", "Electronics & Computers", "Home, Garden & Tools", "Grocery, Health & Beauty", "Toys, Kids & Baby", "Clothing, Shoes & Jewelry", "Sports & Outdoors", and "Automotive & Industrial".

The main content area features a large advertisement for the Kindle, titled "Kindle The #1 Bestseller on Amazon". It displays a Kindle device and lists three models with their prices: Kindle 3G with Special Offers for \$139, Kindle 3G for \$189, and Kindle DX for \$379. Each model has an "Order now" link. Below this is an advertisement for the "Software Download Store" with the text "Get the software you want. Instantly." and a "Learn more" link. To the right of the Kindle ad is an advertisement for "Up to 90% off used textbooks" featuring a stack of books and a "Shop now" link. Below that is an advertisement for the "IMDb Android app" showing a smartphone screen with the app interface and a QR code for downloading. At the bottom right, there is an advertisement for "FREE Two-Day Shipping for Students" with a "Learn more" link.

How about a nice kindle ?

amazon.com

SIGN IN

SHIPPING & PAYMENT

GIFT-WRAP

PLACE ORDER




Review Your Order

By placing your order, you agree to Amazon.com's [privacy notice](#) and [conditions of use](#)

Shipping Address:

Allan Smith
42 GRANT AVE
SAN FRANCISCO, CA 94108-5802
United States
Phone: 666-666-6666 [Change](#)

Billing Information:

 ending in 4444 [Change](#)

Billing Address:

Same as shipping address [Change](#)

Gift Cards & Promotional Codes:

[Apply](#)

[Place your order](#)

Order Summary

Items:	\$139.00
Shipping & Handling:	\$6.98
Total Before Tax:	\$145.98
Estimated Tax To Be Collected:	\$0.00

Order Total: \$145.98

FREE TWO-DAY SHIPPING

FREE Two-Day Shipping on this Order: Allan Smith, you can save \$6.98 on this order by selecting "FREE Two-Day Shipping with a free trial of Amazon Prime" below.

» [Sign up for free trial](#)

Estimated delivery: Aug. 2, 2011



Kindle, Wi-Fi, Graphite, 6" Display with New E Ink Pearl Technology

\$139.00

Quantity: 1 [Change](#)

Sold by: Amazon Digital Services, Inc.

[Add gift options](#)

Choose a shipping speed:

- FREE Super Saver Shipping (5-8 business days)
- FREE Two-Day Shipping with a free trial of **Amazon Prime™** --get it **Saturday, July 30** ([Learn more](#))
- Standard Shipping (3-5 business days)
- Two-Day Shipping --get it **Saturday, July 30**
- One-Day Shipping --get it **Friday, July 29**

By placing your order, you agree to the [Kindle License Agreement and Terms of Use](#).

[How are shipping costs calculated?](#)

How about a nice kindle ?

amazon.com

SIGN IN

SHIPPING & PAYMENT

GIFT-WRAP

PLACE ORDER




Review Your Order

By placing your order, you agree to Amazon.com's [privacy notice](#) and [conditions of use](#)

Shipping Address:

Allan Smith
42 GRANT AVE
SAN FRANCISCO, CA 94108-5802
United States
Phone: 666-666-6666 [Change](#)

Billing Information:

 ending in 4444 [Change](#)

Billing Address:

Same as shipping address [Change](#)

Gift Cards & Promotional Codes:

[Apply](#)

[Place your order](#)

Order Summary

Items:	\$139.00
Shipping & Handling:	\$6.98
Total Before Tax:	\$145.98
Estimated Tax To Be Collected:	\$0.00

Order Total: \$145.98

FREE TWO-DAY SHIPPING

FREE Two-Day Shipping on this Order: Allan Smith, you can save \$6.98 on this order by selecting "FREE Two-Day Shipping with a free trial of Amazon Prime" below.

» [Sign up for free trial](#)

Estimated delivery: Aug. 2, 2011



Kindle, Wi-Fi, Graphite, 6" Display with New E Ink Pearl Technology

\$139.00

Quantity: 1 [Change](#)

Sold by: Amazon Digital Services, Inc.

[Add gift options](#)

Choose a shipping speed:

- FREE Super Saver Shipping (5-8 business days)
- FREE Two-Day Shipping with a free trial of **Amazon Prime™** --get it **Saturday, July 30** ([Learn more](#))
- Standard Shipping (3-5 business days)
- Two-Day Shipping --get it **Saturday, July 30**
- One-Day Shipping --get it **Friday, July 29**

By placing your order, you agree to the [Kindle License Agreement and Terms of Use](#).

[How are shipping costs calculated?](#)

Every form field is recorded

SQLite Database Browser - C:/Users/[redacted]/AppData/Roaming/Mozilla/Firefox/Profiles/s4lqektq.default/formhistory.sqlite

File Edit View Help

Database Structure Browse Data Execute SQL

Table: moz_formhistory

New Record Delete Record

id	fieldname	value	timesUsed	firstUsed	lastUsed	guid
1	1 email	testblackhat@devnull.com		1 1311823018543000	1311823018543000	CTwZ4J59TYySue7B
2	2 enterAddressFullName	Alan Smith		1 1311823235859000	1311823235859000	FXXpcwKuRqSTonB+
3	3 enterAddressAddressLine 1	42 my street		1 1311823235861000	1311823235861000	EFP3mGQES8yz716r
4	4 enterAddressCity	San Fransisco		1 1311823235861000	1311823235861000	/nfoGVLgT4OmGoIQ
5	5 enterAddressStateOrRegion	CA		1 1311823235861000	1311823235861000	n8ckFyg6S3ua8t6Z
6	6 enterAddressPostalCode	94302		1 1311823235862000	1311823235862000	etJpzZGGQ26+2mjq
7	7 enterAddressPhoneNumber	666-666-6666		1 1311823235862000	1311823235862000	H01M4MNTTGu8Oc/f
8	8 enterAddressAddressLine 1	my street		1 1311823259915000	1311823259915000	hj8LVNLgTFug1eDV
9	9 searchbar-history	[redacted]		1 1311823282116000	1311823282116000	poNBcyN2SsydiObN

< 1 - 9 of 9 >

Go to: 0

Configuring a Linksys ?

The screenshot shows the Linksys E4200 web interface for configuring wireless security. The top navigation bar includes the Cisco logo, the device name 'Linksys E4200', and the firmware version '1.0.02'. The 'Wireless' section is active, with sub-tabs for 'Setup', 'Wireless', 'Security', 'Storage', 'Access Restrictions', 'Applications & Gaming', 'Administration', and 'Status'. Under the 'Wireless' tab, there are sub-sections for 'Basic Wireless Settings', 'Wireless Security', 'Guest Access', and 'Wireless MAC Filter'. The 'Wireless Security' section is expanded to show settings for both 5 GHz and 2.4 GHz bands. For each band, the 'Security Mode' is set to 'WPA2/WPA Mixed Mode' and the 'Passphrase' is 'thisismywpakey'. At the bottom of the configuration area, there are 'Save Settings' and 'Cancel Changes' buttons. A 'Help...' link is visible on the right side of the page.

Again the key is recorded

The screenshot shows the SQLite Database Browser interface. The title bar indicates the database path: C:/Users/.../AppData/Roaming/Mozilla/Firefox/Profiles/s4lqektq.default/f... The menu bar includes File, Edit, View, and Help. The toolbar contains icons for file operations and database actions. The main area shows the 'Browse Data' tab selected, with the table 'moz_formhistory' chosen. A single record is displayed in a table with the following columns and values:

id	fieldname	value	timesUsed	firstUsed	lastUsed	quid
1	wl0_wpa_psk	thisismywpakey		1 1311824553188000	1311824553188000	cw7acN7

At the bottom, there are navigation buttons for record selection (1 - 1 of 1) and a 'Go to:' field with the value 0.

Form history leak a lot of information

- Shipping address
- Wifi key
- Credit card information
- Email
- Search history



Preventing field recording

To tell the browser to not record a field use the tag

`autocomplete="off"`



Internet
Explorer

- Passwords
 - Location: **registry**
 - Encryption: **DPAPI + URL as salt**
- History
 - URLs: **Index.dat**

Decrypting Internet Explorer passwords

Decrypting Internet Explorer passwords

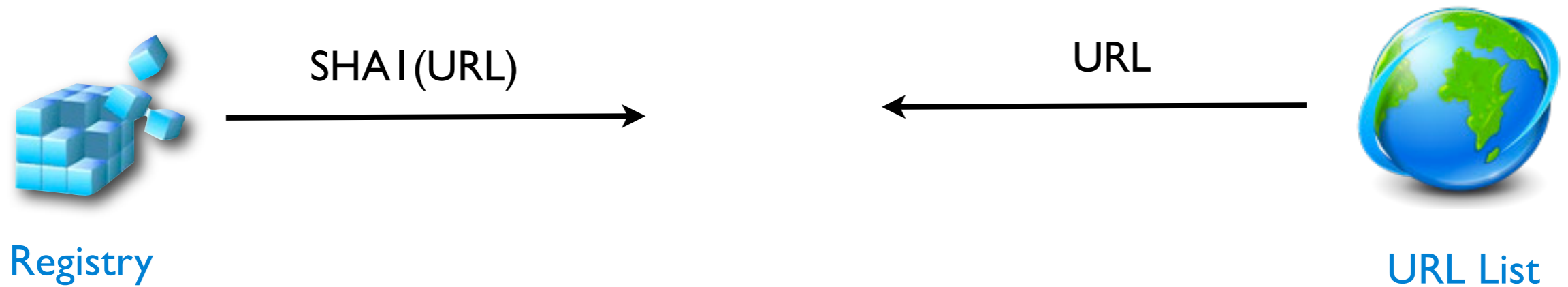


Registry

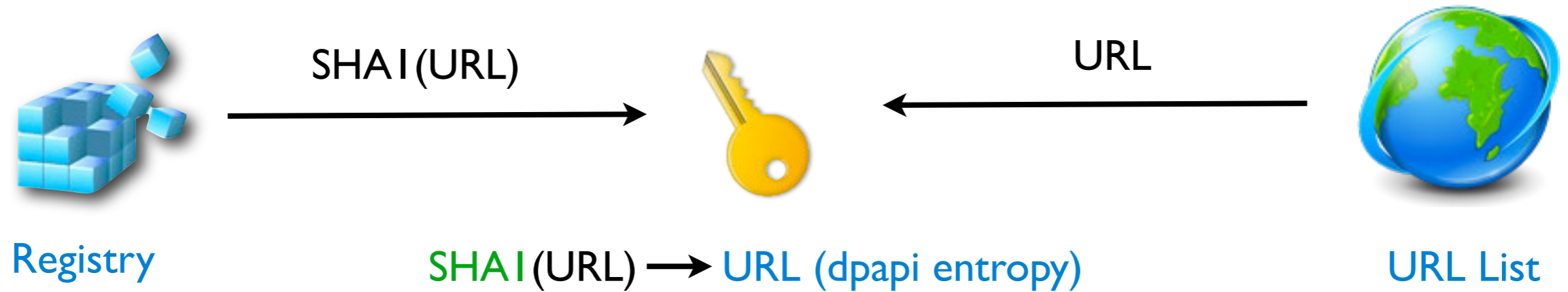
SHA1(URL)



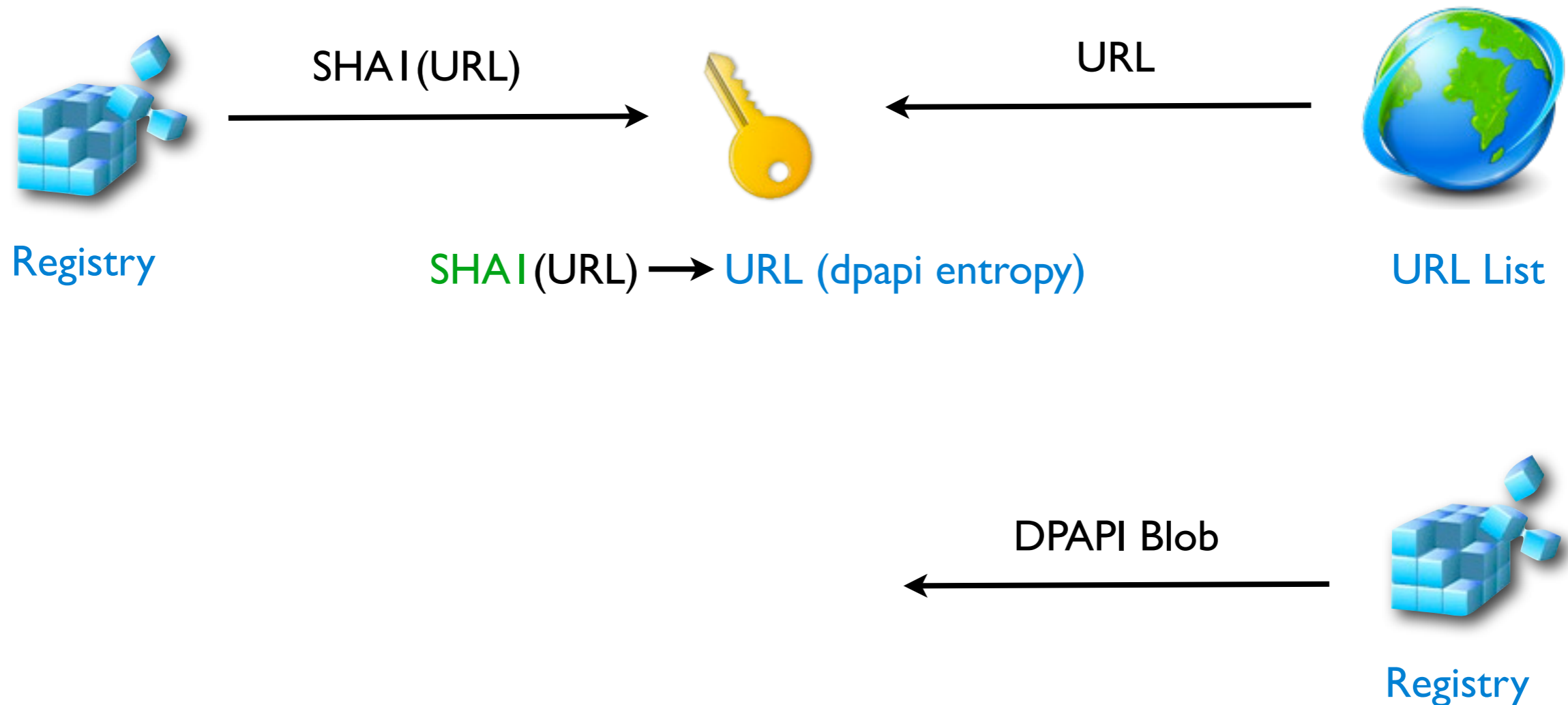
Decrypting Internet Explorer passwords



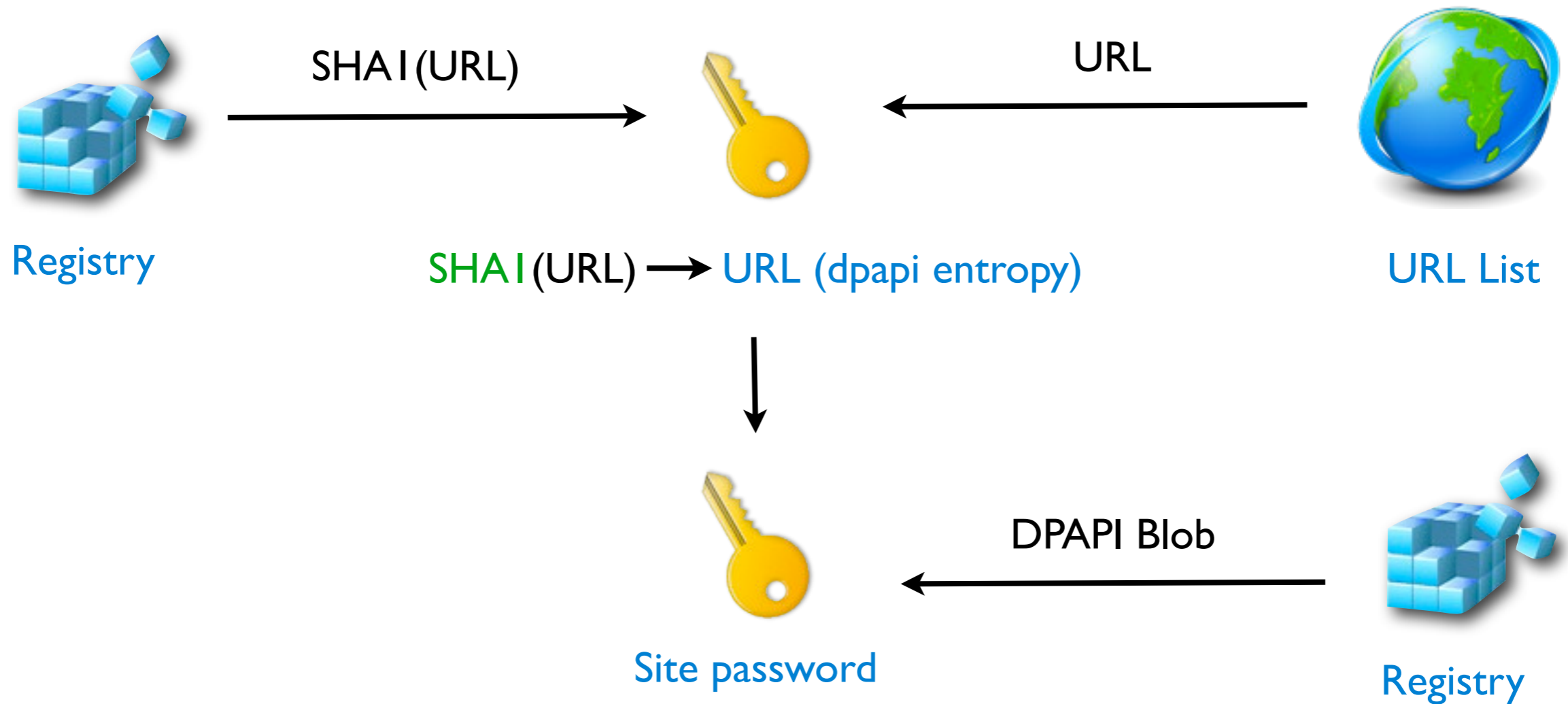
Decrypting Internet Explorer passwords



Decrypting Internet Explorer passwords



Decrypting Internet Explorer passwords



Maximizing our recovery

- Build a list of URL from others browsers and files
- Use a list of known login URLs



Chrome

- Passwords
 - Location: **Login Data (sqlite)**
 - Encryption: **DPAPI**
- History
 - URLs: **History (sqlite)**
 - Forms fields: **Web Data (sqlite)**



Safari

- Passwords
 - Location: **keychain.plist** (Property list format)
 - Encryption: **DPAPI** + fixed string as entropy
- History
 - URLs: **History.plist**
 - Forms fields: **Form Value.plist**

Browsers takeaway

- Internet Explorer is the most secure.
 - If you don't know the URL you can't recover the credentials
- Firefox is the worst
 - Passwords encryption not tied to the Windows user password (bug open for a while)
 - Logins are encrypted in signons.sqlite not in formhistory.sqlite



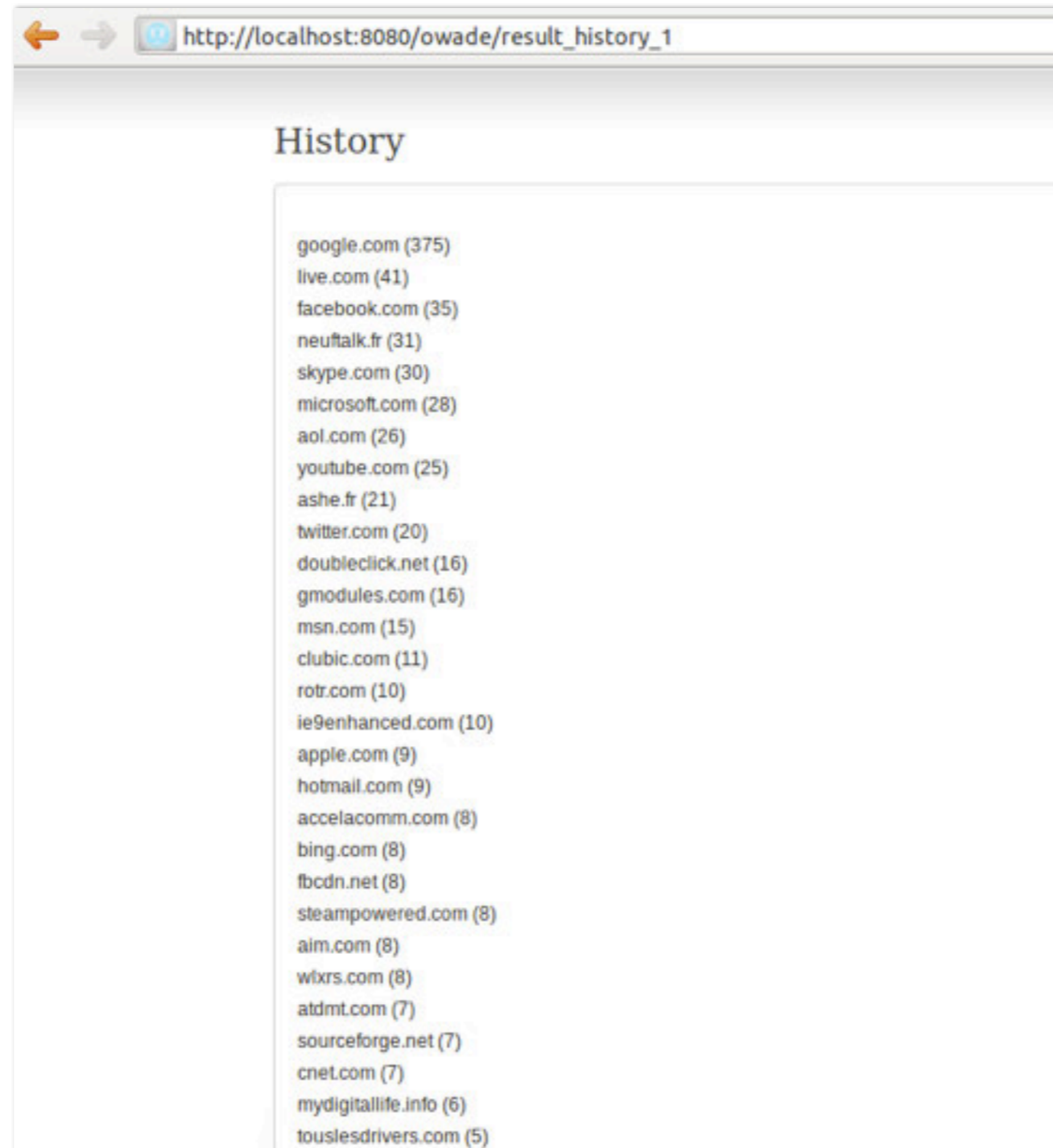
Private mode

- Most bugs are fixed
- Requires to be creative
 - SSL OCSP requests
 - File carving
- Potential techniques
 - Analyze the hibernate file



See: <http://ly.tl/p16> for more information on private mode

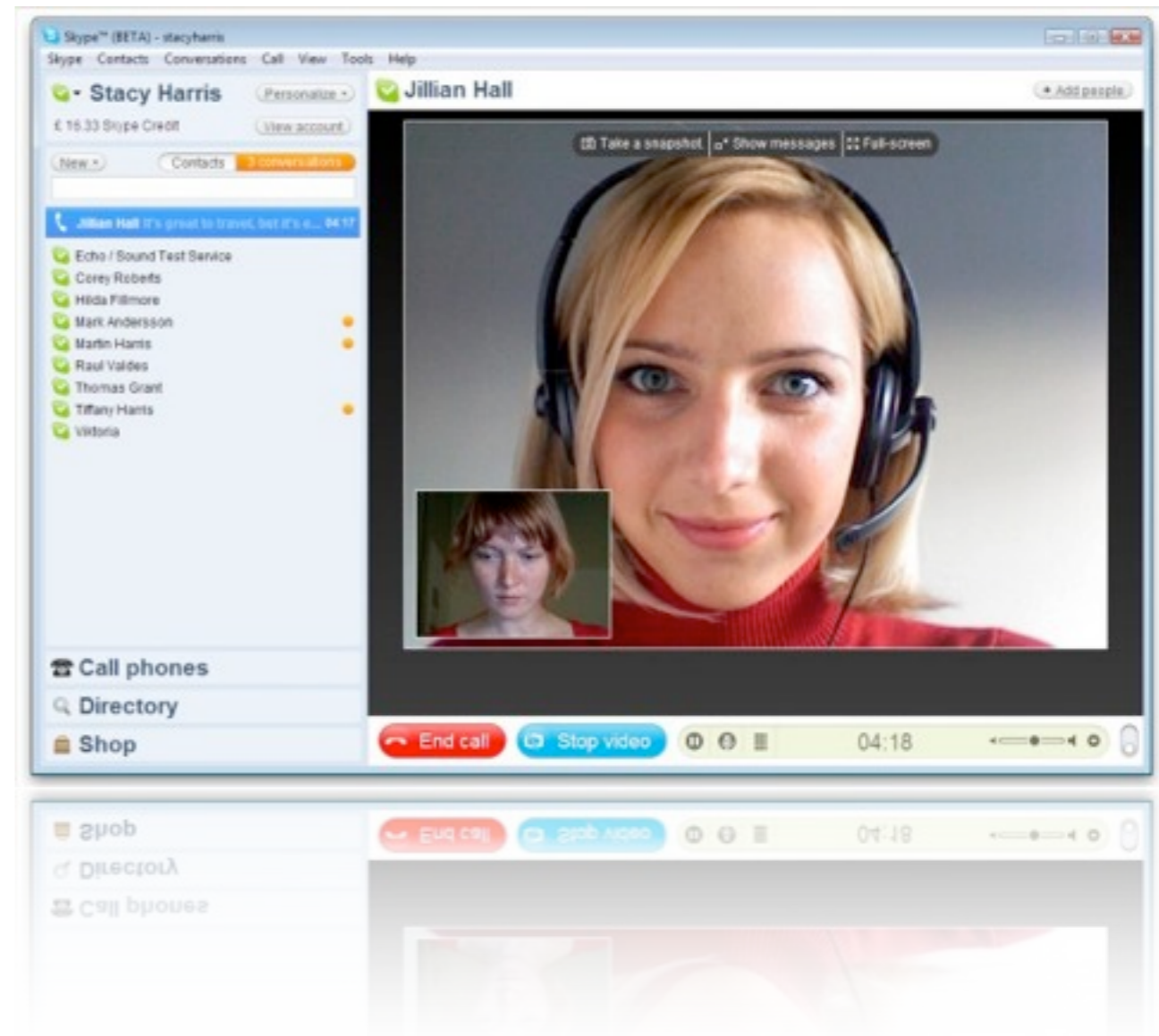
The browsers histories aggregated



Instant messaging

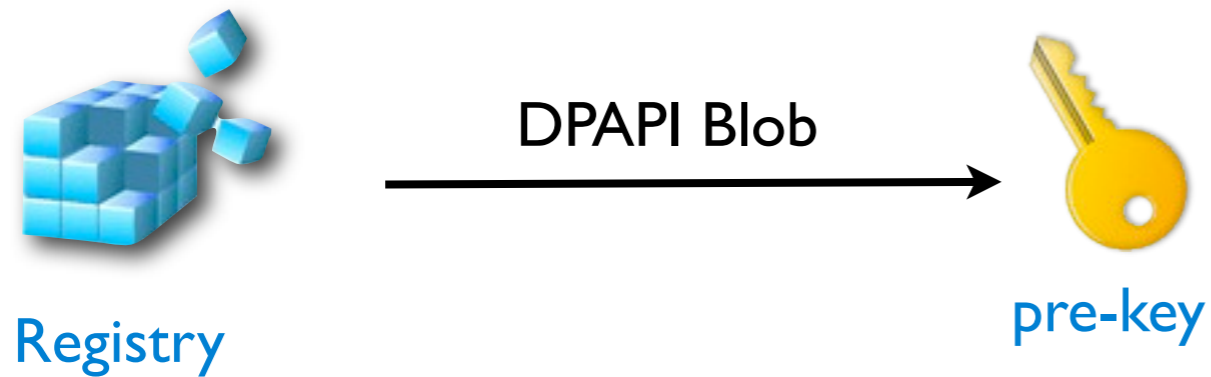
Skype

- Encryption
custom
- Difficulty
extreme
- Location
registry + config.xml



Decrypting Skype passwords

Decrypting Skype passwords

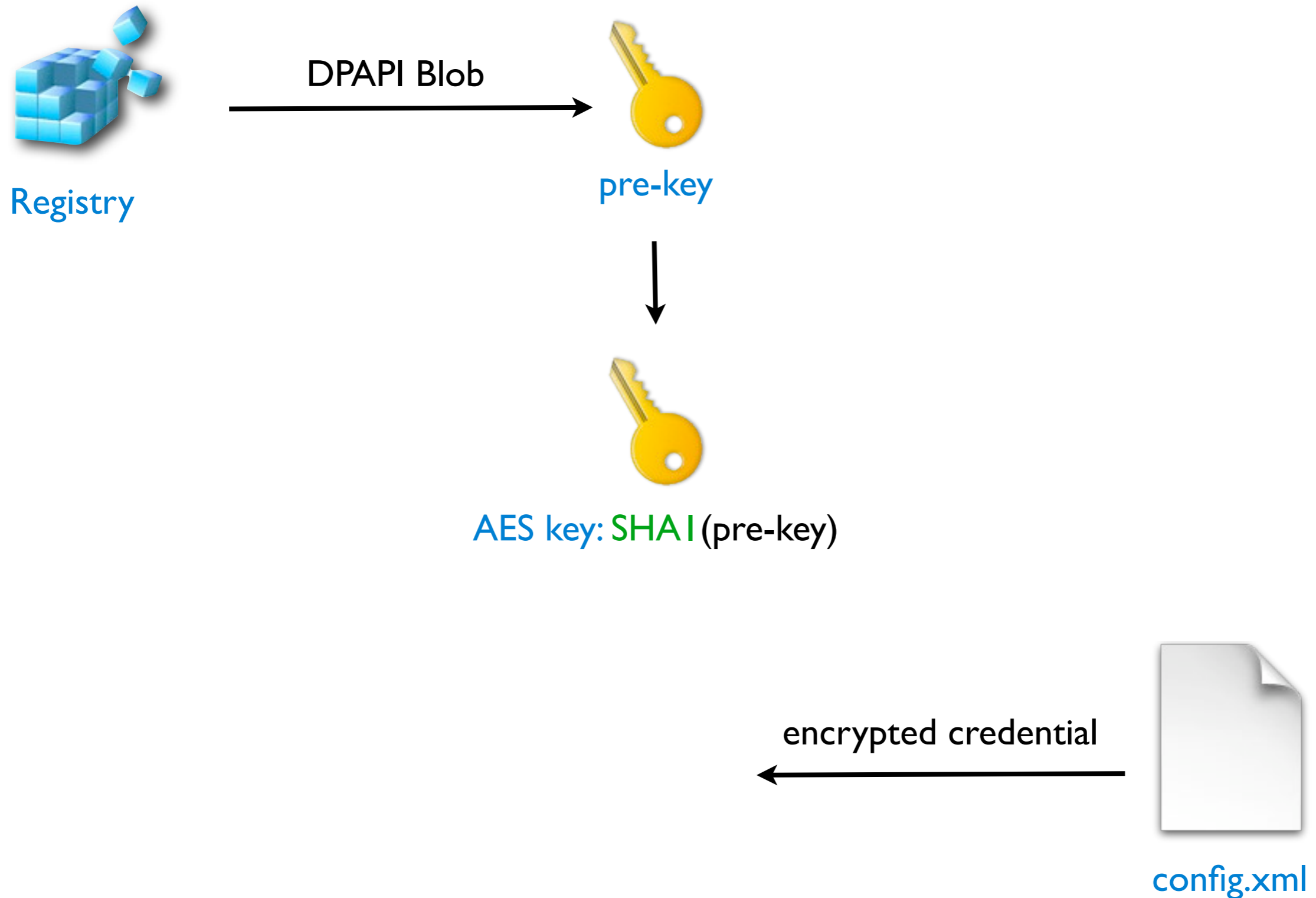


Decrypting Skype passwords

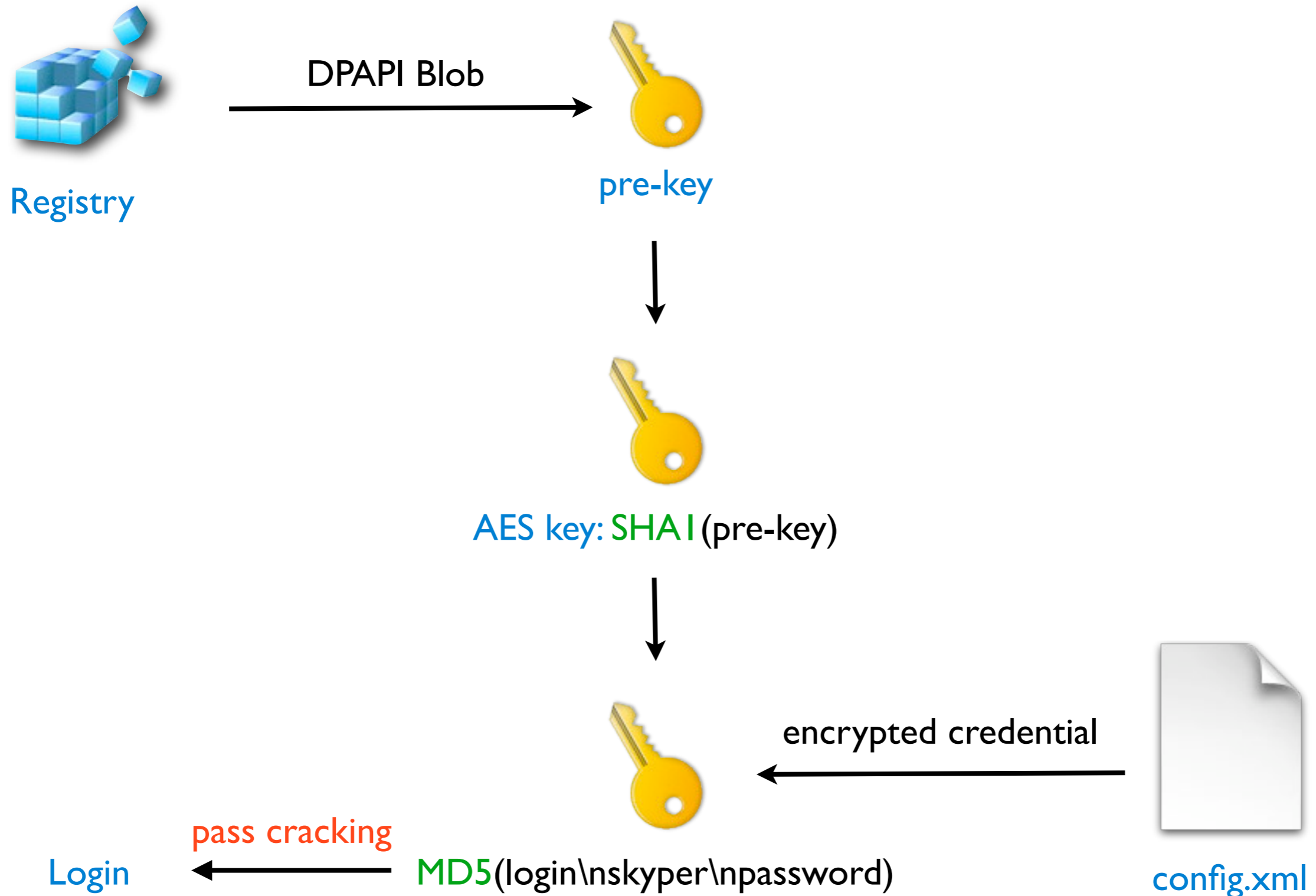


AES key: **SHA1** (pre-key)

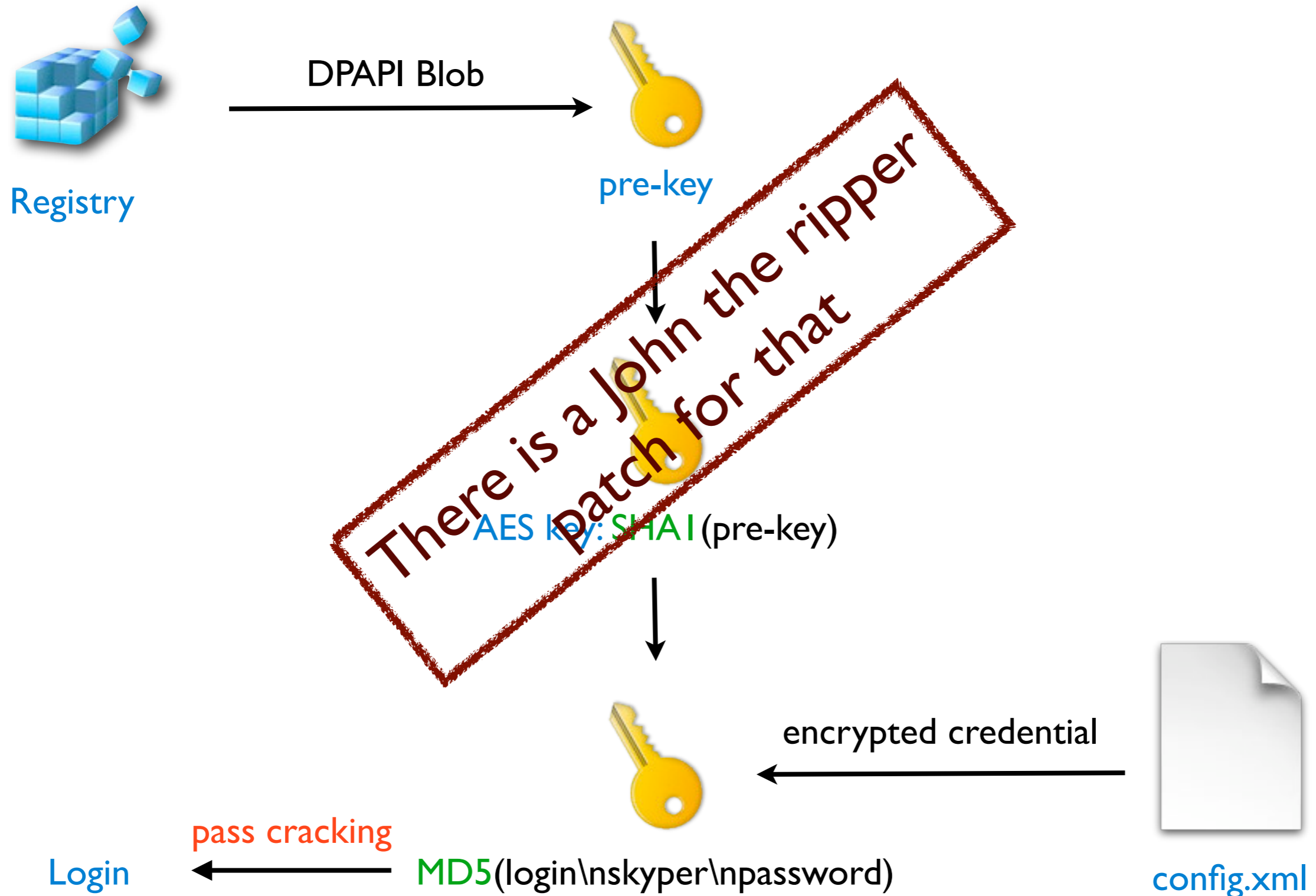
Decrypting Skype passwords



Decrypting Skype passwords

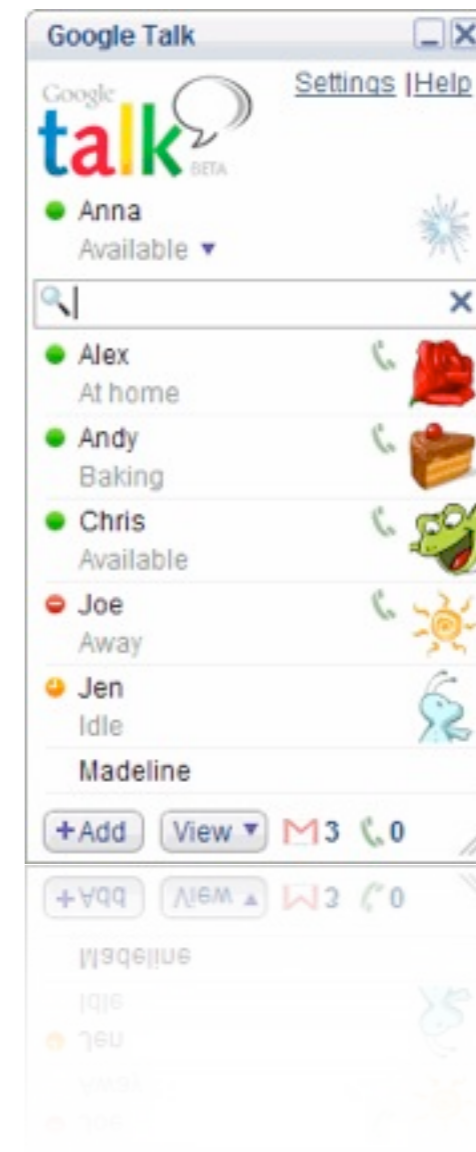


Decrypting Skype passwords




Google Talk

- Encryption
DPAPI + custom (salt)
- Difficulty
Hard
- Location
registry



Salt derivation algorithm overview

Salt derivation algorithm overview

String: 0xBA0DA71D


Salt derivation algorithm overview

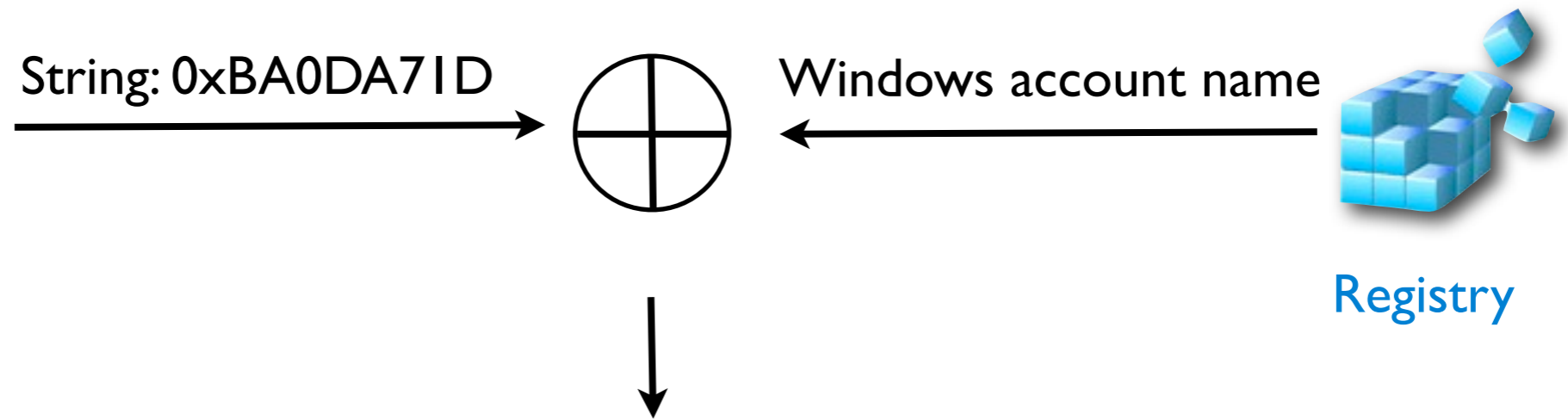
String: 0xBA0DA71D
→

← Windows account name

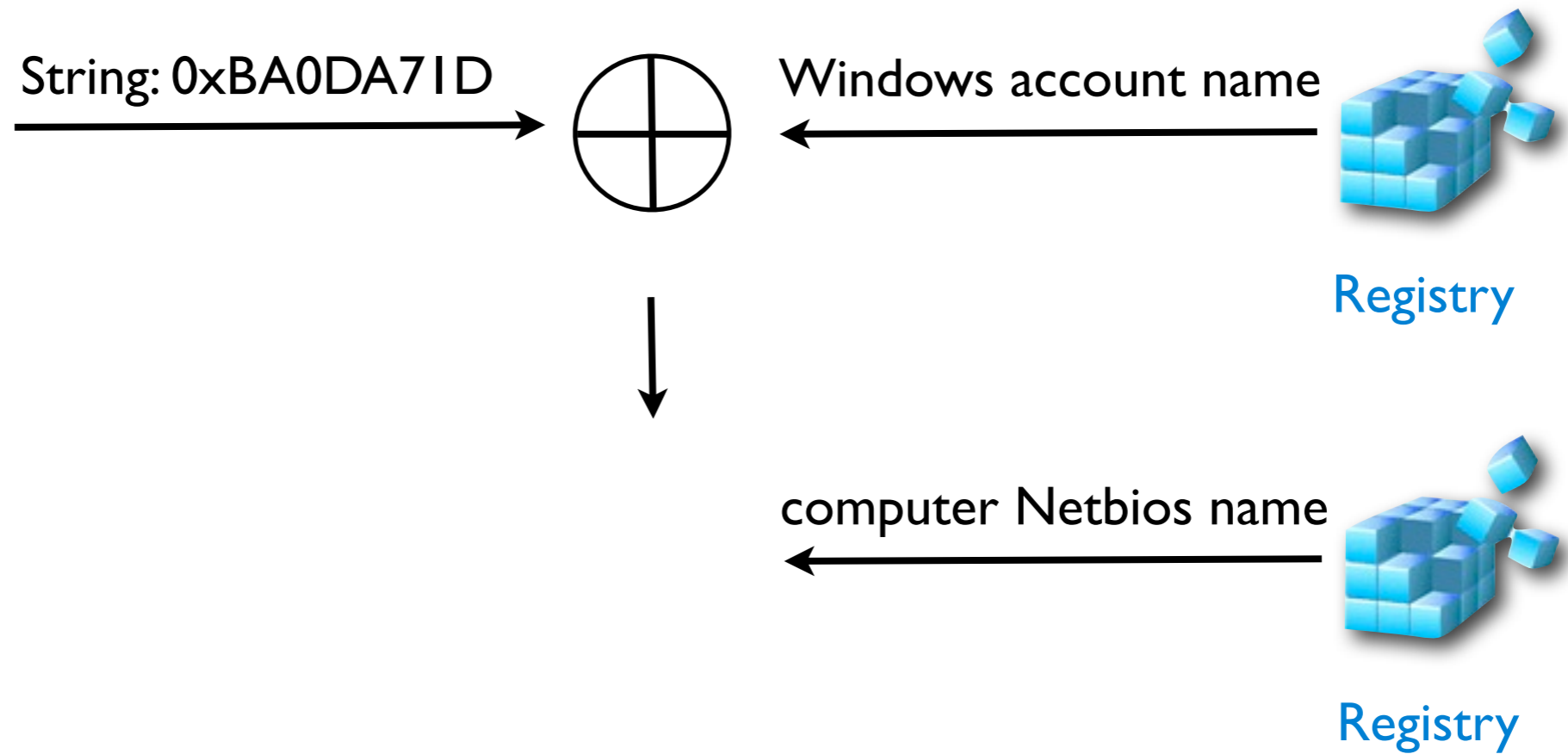


Registry

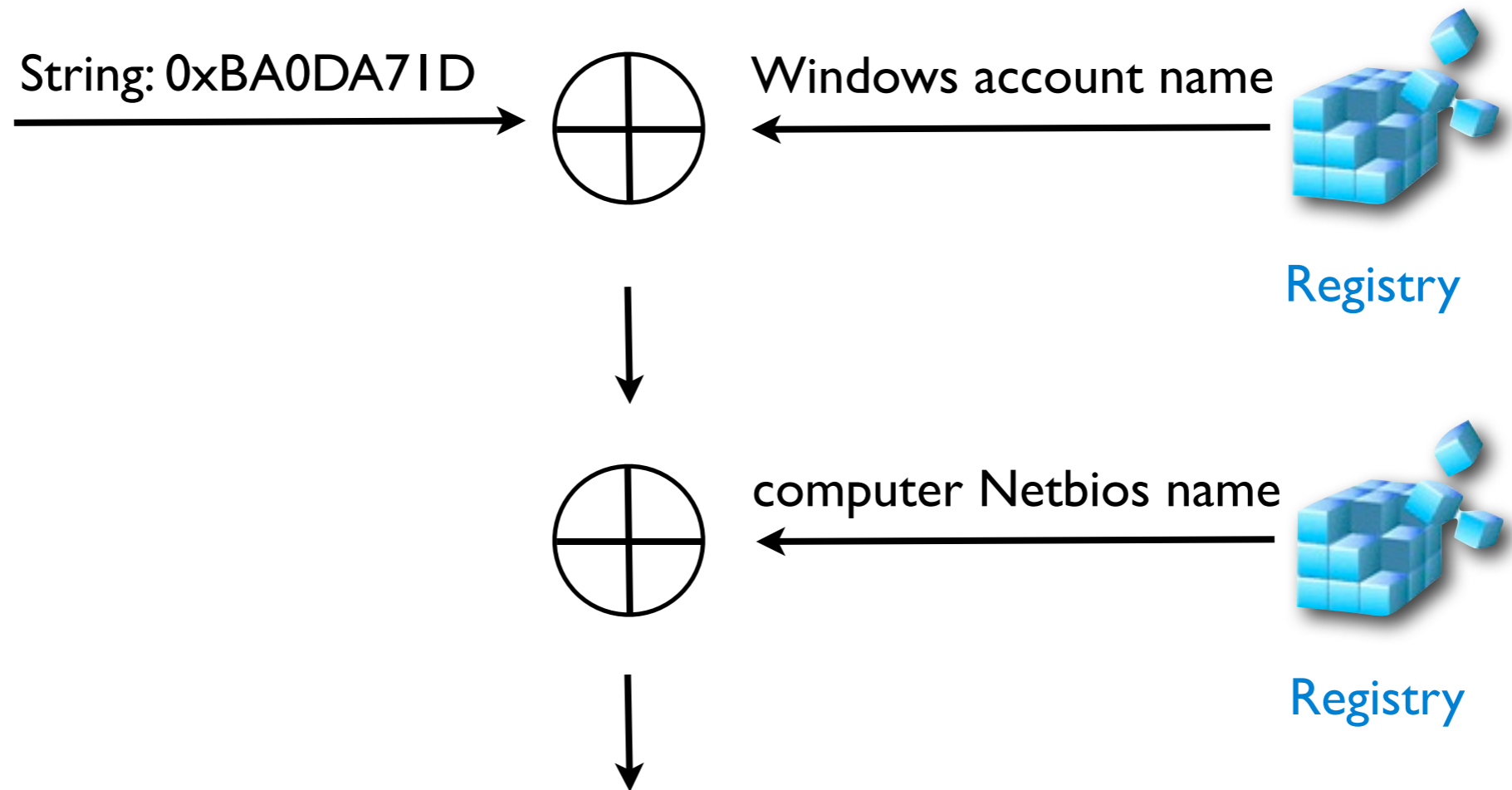
Salt derivation algorithm overview



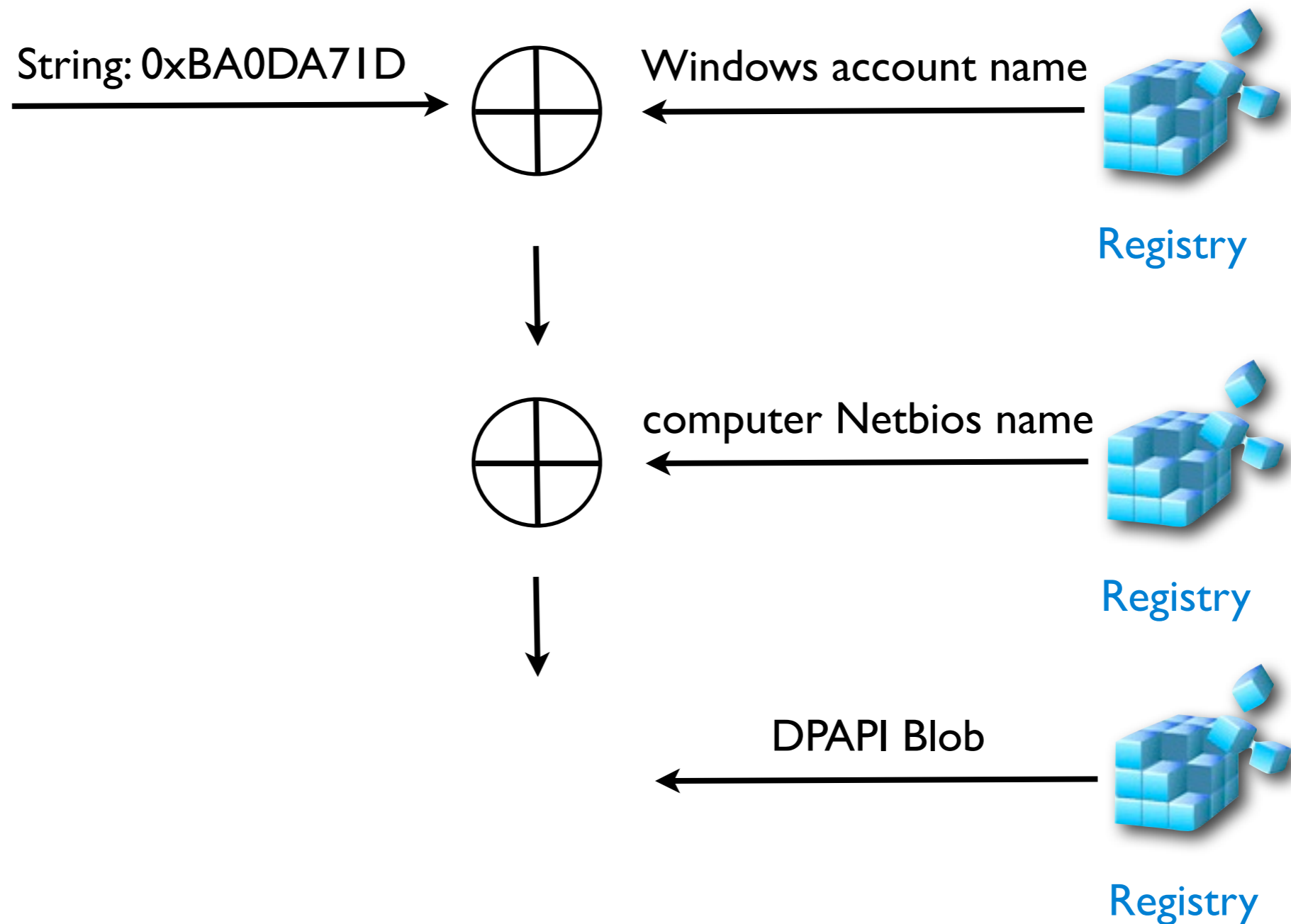
Salt derivation algorithm overview



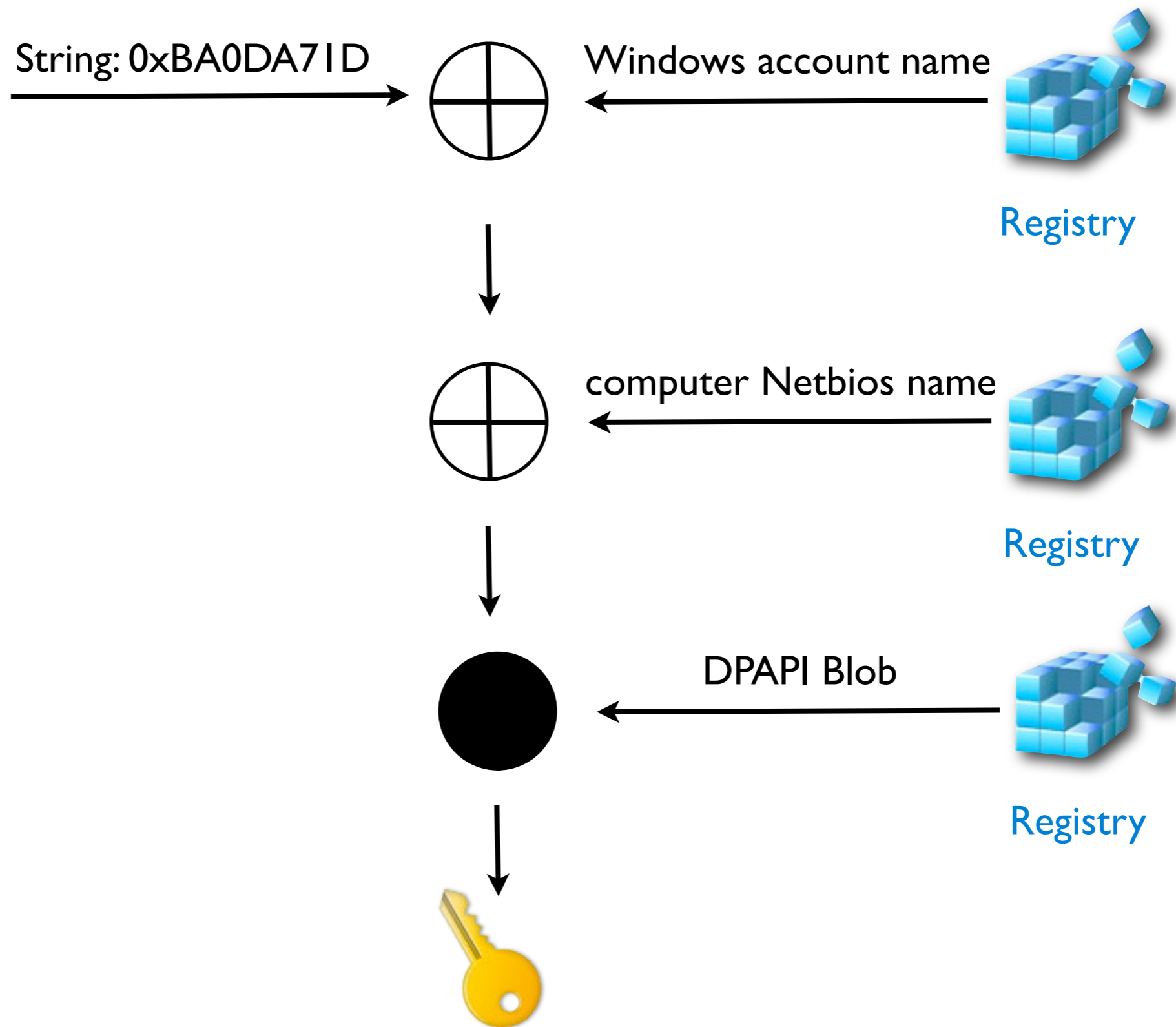
Salt derivation algorithm overview



Salt derivation algorithm overview

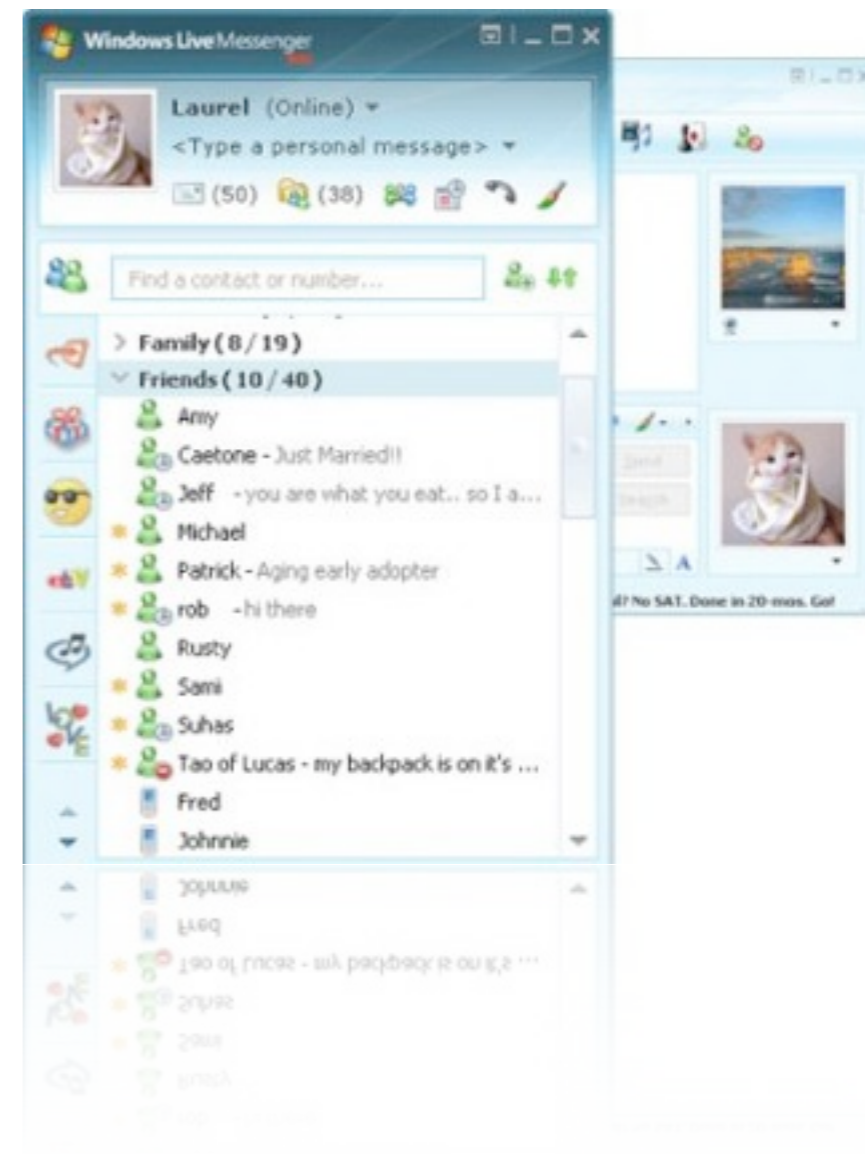


Salt derivation algorithm overview



Microsoft Messenger

- Encryption
DPAPI or Credstore
- Difficulty
Medium
- Location
version dependent



Windows Messenger by version

Version	Storage	encryption
5	Registry	Base64 encoded
6	Credstore	Credstore
7	Registry x2	DPAPI x 2
Live	Credstore	Credstore

- Encryption

DES

key: substr(login .“dummykey”, 8)

- Difficulty

easy

- Location

config.xml

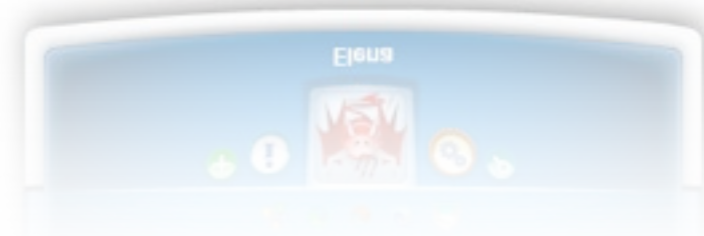


- Encryption
XOR
key: 9
- Difficulty
trivial
- Location
user.config



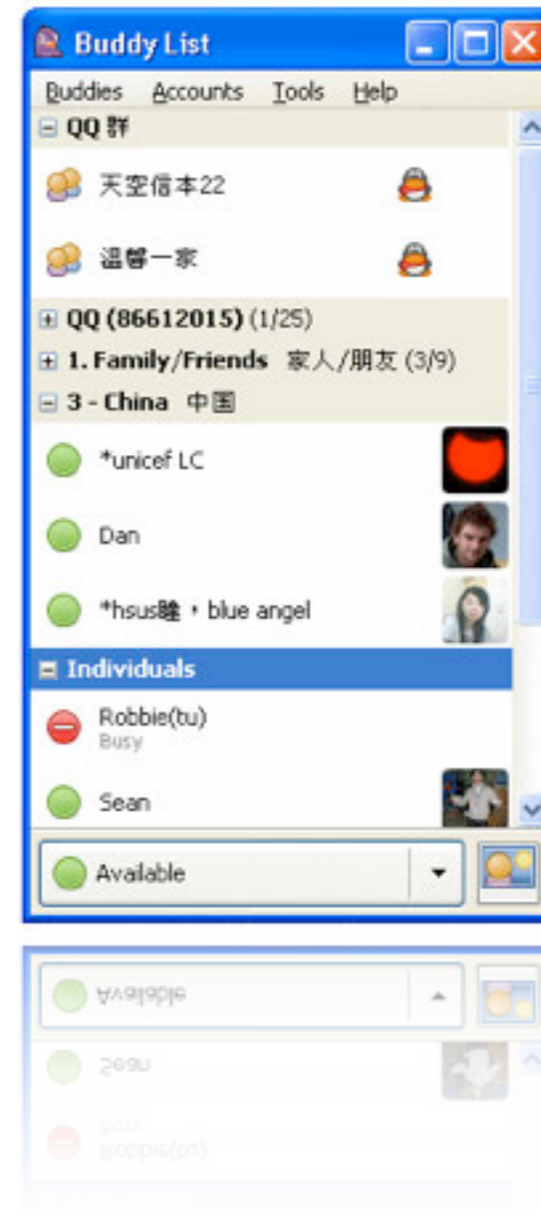
Trillian

- Encryption
Base 64 +XOR
key: fixed string
- Difficulty
trivial
- Location
user.config



Pidgin

- Encryption
Clear aka encrypt-what?
- Difficulty
none
- Location
account.xml



Pidgin

- Encryption
Clear aka encrypt-what?
- Difficulty
none
- Location
account.xml

Paltalk

- Encryption
Custom
- Difficulty
difficult (offline)
- Location
registry



Paltalk encryption algorithm

Paltalk encryption algorithm

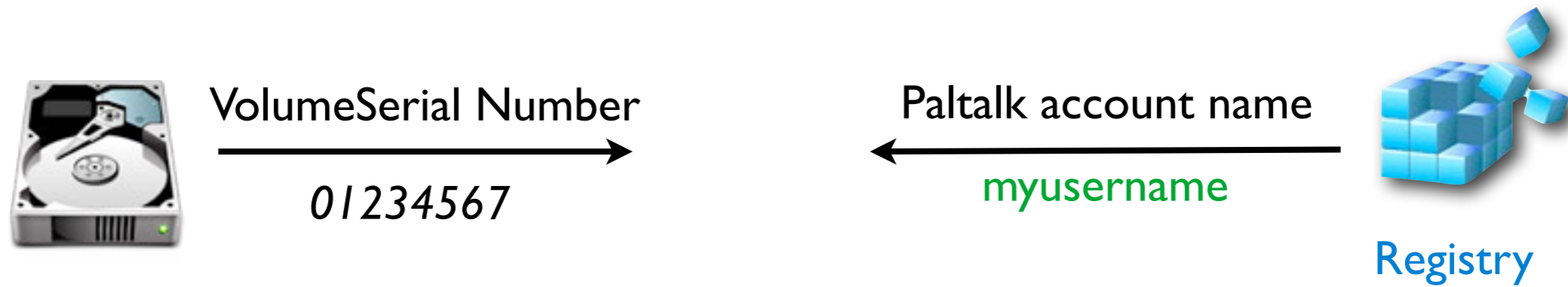


VolumeSerial Number

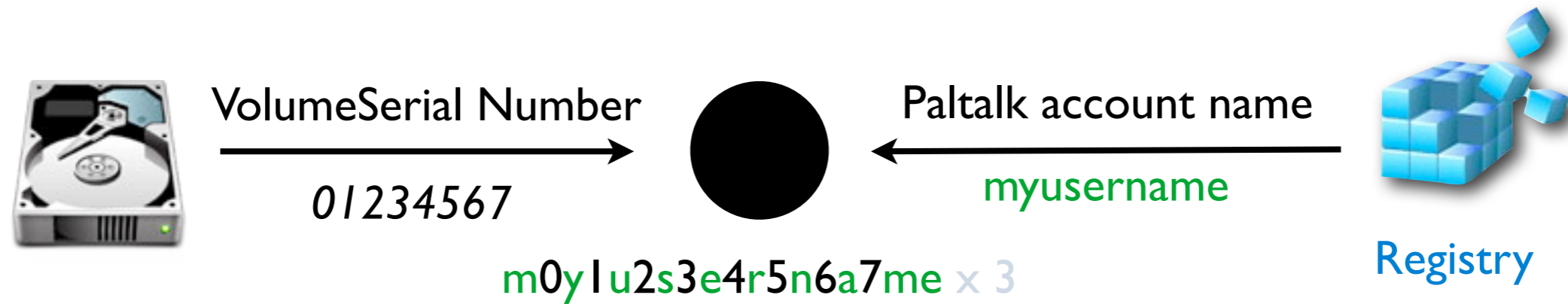


01234567

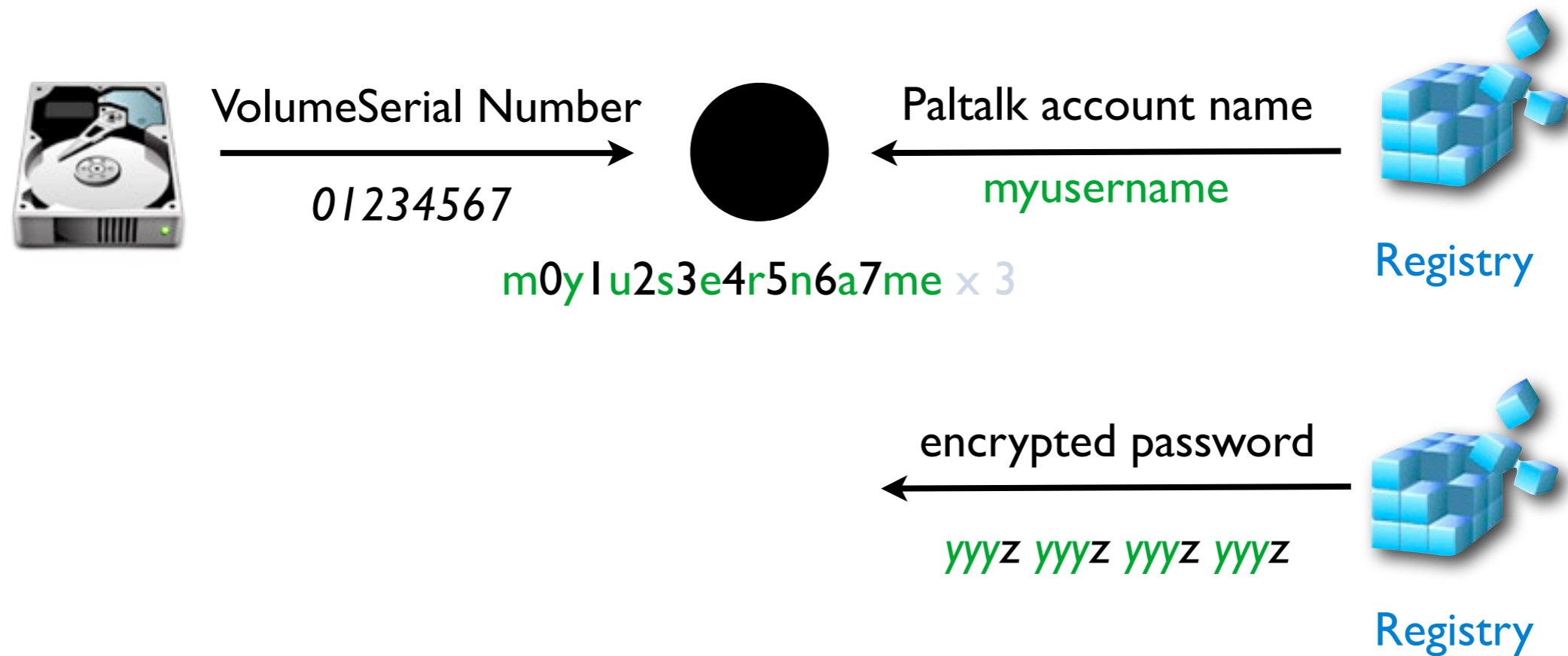
Paltalk encryption algorithm



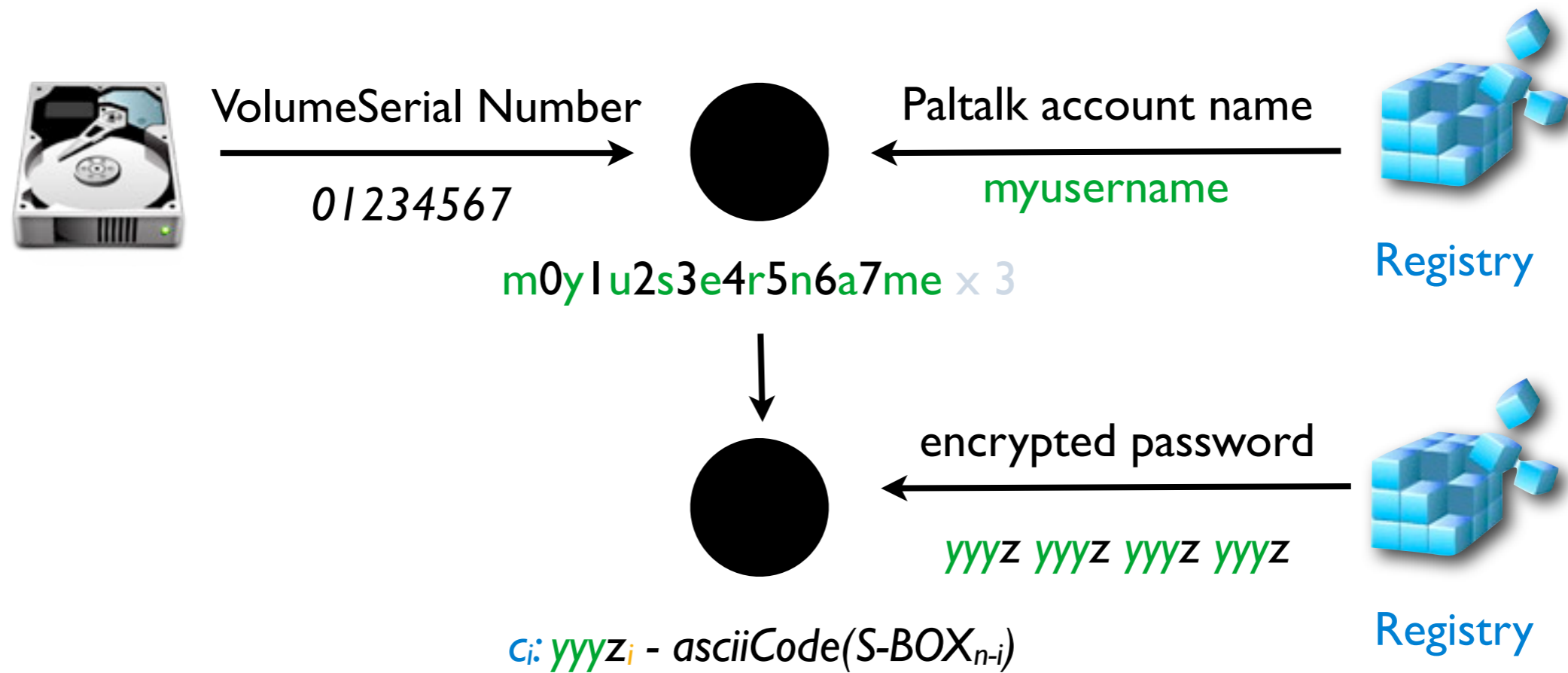
Paltalk encryption algorithm



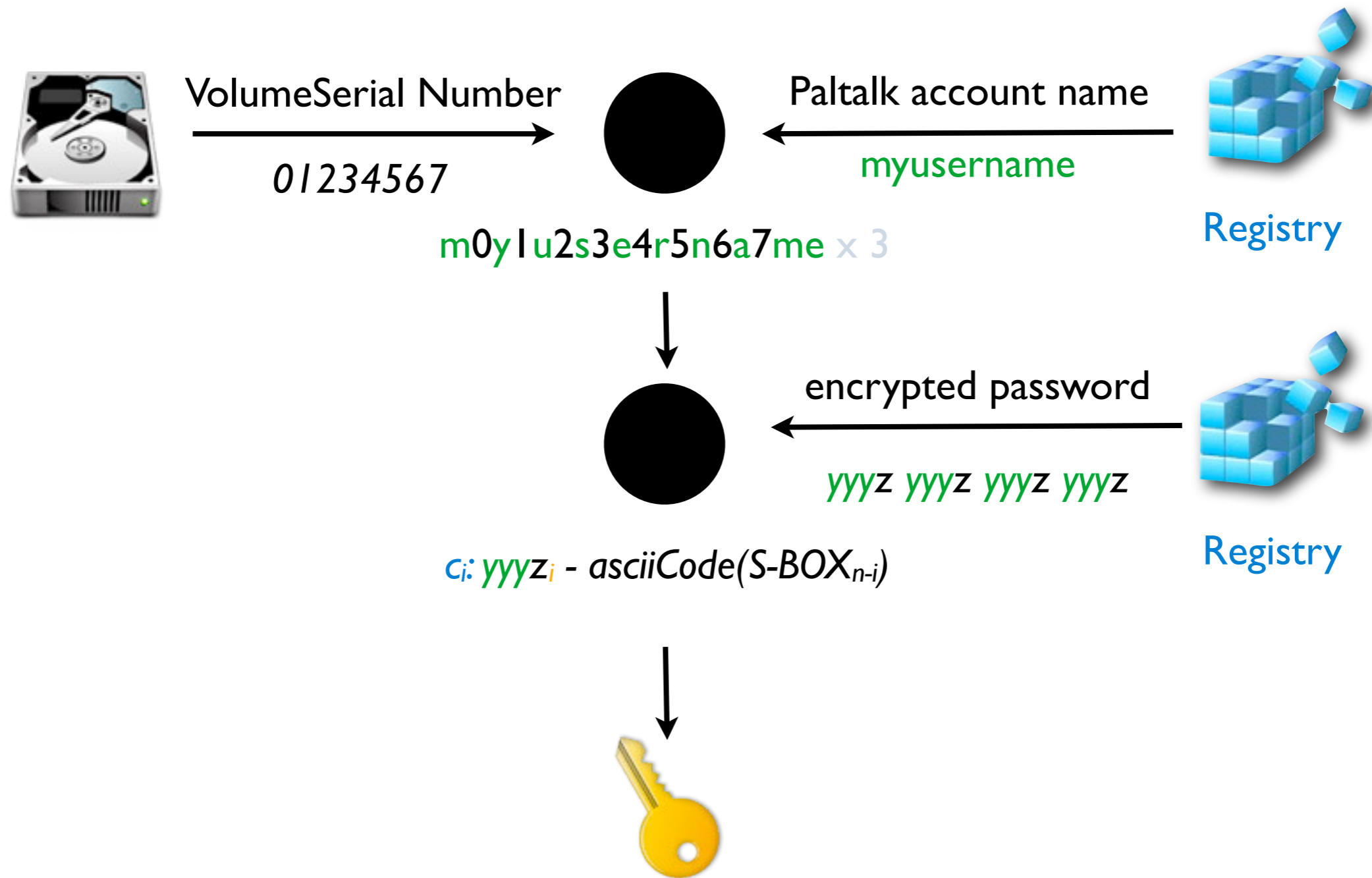
Paltalk encryption algorithm



Paltalk encryption algorithm




Paltalk encryption algorithm



Messenger take away

- If your Skype password is strong we **can't recover it**
- Gtalk and Paltalk are the **only ones** to use computer information
- **3rd party** software are the **least secure**

All the credentials recovered by OWADE

← →  http://localhost:8080/owade/result_passwords_1

Chrome
Login: owade
Password: rootroot
Domain: ashe.fr

Chrome
Login: project.owade
Password: rootroot
Domain: google.com

Safari
Login: owade
Password: rootroot
Domain: ashe.fr

Trillian
Login: project.owade
Password: rootroot

GTalk
Login: project.owade@gmail.com
Password: rootroot

Most used

Passwords
rootroot

Usernames
owade
project.owade



Cloud based forensic

Cloud modules

- Leverage the credentials and history extracted to get cloud-data
- Might be legal (or not)
- Only LinkedIn currently (more modules almost ready)

The image shows a screenshot of a LinkedIn profile for Elie Bursztein. The profile is for a 'Basic' account type. The header includes navigation links: Home, Profile, Contacts, Groups, Jobs, Inbox, Companies, News, and More. The profile picture is a headshot of Elie Bursztein. The bio identifies him as a 'Researcher at Stanford University' in the 'San Francisco Bay Area' with a focus on 'Research'. A recent activity post from 10 minutes ago mentions 'Beyond files recovery, OWADE cloud-based forensic are available for download.' The 'Current' role is 'Researcher at Stanford University'. Past roles include 'Instructor at PGSM', 'CEO at Option Saft', and 'Professor at Epita'. Education includes 'Ecole Normale Supérieure de Cachan', 'Université Denis Diderot (Paris VII)', and 'Ecole pour l'Informatique et les Techniques Avancées'. He has 276 connections. Websites listed are 'Personal Website', 'Blog', and 'My Research Group'. His Twitter handle is 'elie' and his public profile URL is 'http://www.linkedin.com/in/bursztein'. The 'Summary' section describes his expertise in CAPTCHAs, web security, mobile security, and machine learning. The right sidebar shows 'Elie's Activity' with several recent posts, including one about geolocation API and another about tracking users.

OWADE status

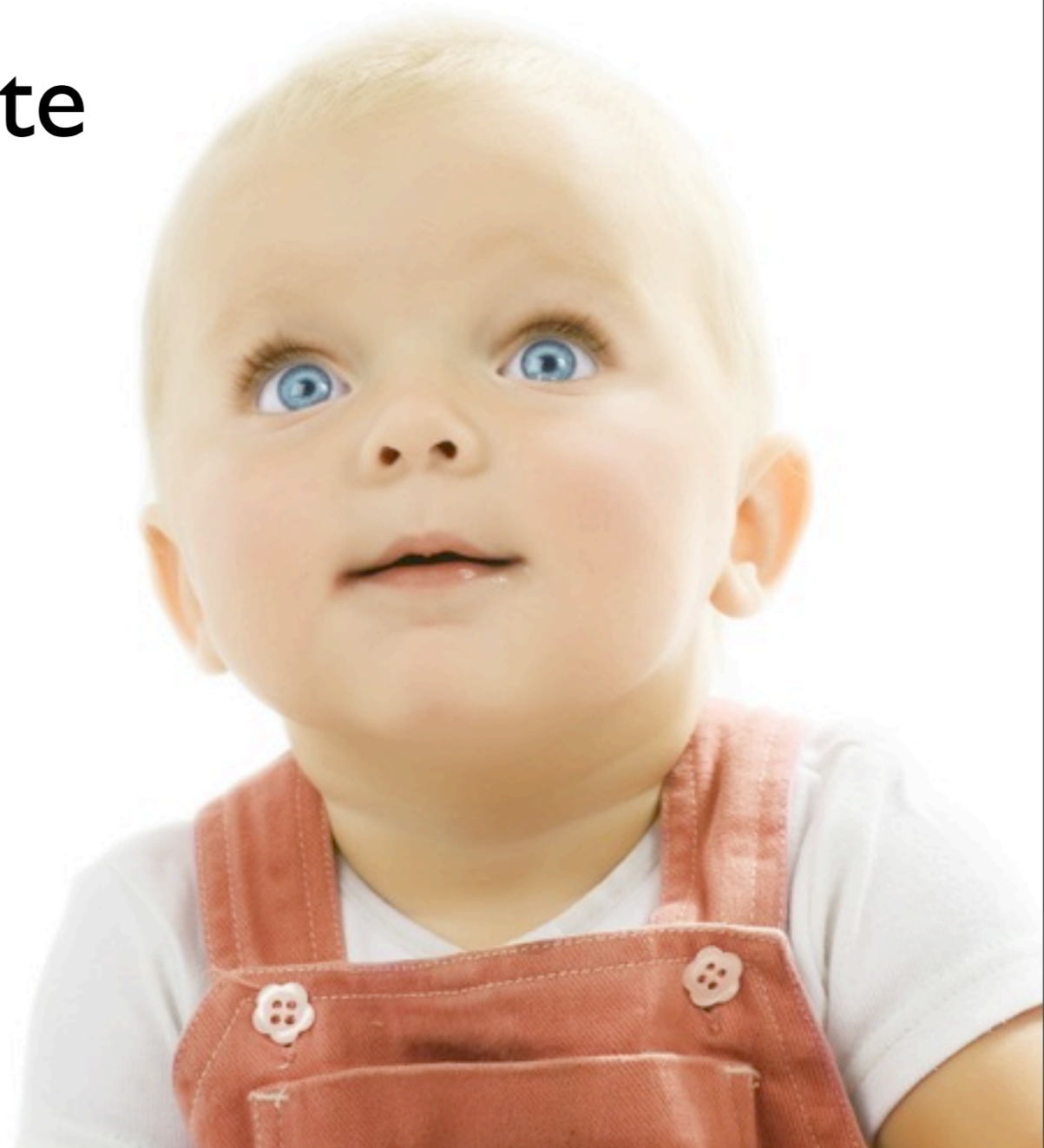
- Alpha stage
 - Tested on Ubuntu against XP windows
- Roadmap
 - Stabilizing the code
 - modularize the code so you write your own modules
 - More cloud probes: Facebook, Flickr, Emails...
 - Windows Vista and 7 integration

Conclusion

- People moving to the cloud means **more data** that is **harder to get**
- Forensics needs to evolve to cope with this
- OWADE is the first tool dedicated to cloud forensic
 - Decrypt the 4 major browsers data
 - Decrypt Instant messaging credentials
 - Open-source

Thank you !

Please remember to complete
your feedback form :)





Download OWADE
<http://owade.org>

Follow-us on Twitter
[@elie](#), [@projectowade](#)

Donate to OWADE to support it !