

~~Anonym surfning~~ och säkra klienter

.se | internetdagarna 2011-11-22

Andreas Jonsson
andreas@romab.com

Tobias Norrbom
tobias@romab.com

▶ www

▶ mail

▶ im

▶ irc

Information

- ▶ från trovärdiga källor
- ▶ spam
- ▶ phishing

Mail

▶ trovärdiga källor

▶ fallgropar

◆ ad nätverk

◆ iframes

◆ flash

▶ internet explorer

▶ firefox

▶ chrome

▶ safari

▶ opera

webbläsare

► uppdateras allt fortare

- ◆ flera versioner underhålls parallellt
- ◆ användare tror oftast att bara den senaste gäller
- ◆ vi är på väg bort från versionsnummer

webbläsares version

▶ vanlig surf

◆ valfri läsare

▶ myndighetssurf

◆ INTE valfri läsare

val av webbläsare

► csn

◆ e-legitimation

◆ personlig kod

Välj inloggningssätt

För den tjänst du har valt kan du välja mellan att logga in med din e-legitimation eller din personliga kod från CSN.

Har du problem att logga in? Läs mer under Vanliga frågor i menyn till vänster.

Om du har Telias e-legitimation och Mac och använder Safari 5 kan det vara problem att logga in. Har du möjlighet kan du pröva att använda Firefox i stället. [Läs mer](#)

Logga in med e-legitimation

Med e-legitimation kan du använda alla tjänster i Mina sidor.

- BankID
- Nordea
- Telia

Logga in med personlig kod från CSN

- Personlig kod
- Beställ personlig kod

▶ skatteverket

◆ e-legitimation

Skriv ut personbevis

Tjänsten är öppen varje dag mellan klockan 07:00-24:00. Måndagar mellan klockan 20:00-20:15 är tjänsten stängd för tekniskt underhåll.

Logga in med legitimation från

- [BankID](#)
- [Nordea](#)
- [SEB eller Telia](#)

myndigheter

ROMAB
Robert Malmgren AB

- ▶ försäkringskassan
 - ◆ e-legitimation

Logga in



Skriv ut

Logga in med e-legitimation från:

- [BankID](#) Läs mer om vilka banker som erbjuder BankID under länken Ladda ner e-legitimation.
- [Nordea](#)
- [Telia](#) ICA Banken, Posten, SEB, Skatteverket

myndigheter

► pensionsmyndigheten

◆ e-legitimation

◆ personlig kod



Logga in på Dina pensionssidor

- Välj inloggning -

- Välj inloggning -

- E-leg: BankID
- E-leg: Nordea
- E-leg: SEB
- E-leg: Telia
- Personlig kod

[Mer om myndigheten](#)

myndigheter

- ▶ rekryterings myndigheten
 - ◆ personlig kod

The image shows a screenshot of a web form titled "Logga in". It contains two input fields: "Personnummer:" with a placeholder "ååååmmdd-xxxx" and "Personlig kod:". Below the fields is a "Logga in" button.

Nordea

TELIA

Danske Bank

Handelsbanken

skandia : banken

Länsförsäkringar

IKANO
BANK

BankID

SPARBANKEN
ÖRESUND

Sparbanken Syd

Swedbank
och Sparbankerna

TELIA genom SEB

TELIA genom ICA Banken

- ▶ nordea
- ▶ telia
- ▶ bank id

e-legitimation

ROMAB
Robert Malmgren AB

► rekommenderar den SENASTE säkerhetsuppdateringen

| Operativsystem | Rekommenderade webbläsare |
|----------------|---------------------------|
| Windows XP | Internet Explorer 7 - 9* |
| Windows Vista | Mozilla Firefox 8 |
| Windows 7 | Google Chrome 15 |
| Mac OS X 10.5 | Mozilla Firefox 3.6* |
| Mac OS X 10.6 | |
| Mac OS X 10.7 | |

* Använd 32-bitars för din webbläsare.

► rekommenderar UPPDATERADE program

| | Firefox 3.0.7 och senare | Firefox 4 och senare ** | Safari 4 och senare | Google Chrome | Internet Explorer 7 | Internet Explorer 8 | Internet Explorer 9 |
|---|-----------------------------------|----------------------------------|---------------------------|------------------|---------------------------|---------------------------|---------------------------|
| Windows XP | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | |
| Windows Vista 32-bit | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Windows Vista 64-bit | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | | (32-bit)* | (32-bit)* | (32-bit)* | (32-bit)* | (32-bit)* | (32-bit)* |
| Windows 7 32-bit | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ |
| Windows 7 64-bit | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ |
| | | (32-bit)* | (32-bit)* | (32-bit)* | | (32-bit)* | (32-bit)* |
| Mac OS X 10.5 | ✓ | ✓ | ✓ | ✓ | | | |
| Mac OS X 10.6 & 10.7 | ✓ | ✓ | ✓** | ✓ | | | |
| Linux Ubuntu 32-bit 10.04 och senare | ✓ | | | ✗ | | | |

* 32-bitars version av webbläsare krävs

** BankID säkerhetsprogram måste uppdateras till senaste version

► rekommenderar inget

Operativsystem

För att du ska kunna använda din e-legitimation korrekt bör du ha något av följande operativsystem:

- MS Windows: XP (endast 32 bitars), Vista (32 och 64 bitars) eller Windows 7 (32 och 64 bitars)
- Mac: Mac OS X version 10.5 (Leopard), 10.6 (Snow Leopard, 32 och 64 bitars), 10.7 (Lion)
- Linux: Ubuntu 10.04 och 10.10

Webbläsare

För användning av Telia e-legitimation stöds följande webbläsare:

- MS Windows: 32-bitarsversioner av Internet Explorer 7.0, 8.0 och 9.0 samt Firefox 3.5, 3.6, 4 och 6
- Mac: Safari 5, 5.1 samt Firefox 3.5, 3.6, 4 och 6
- Ubuntu: Firefox 3.5, 3.6, 4 och 6

Hur vet jag vilken version av Firefox som är installerad på datorn?

- Windows - Öppna ett Firefox fönster. Klicka på Hjälp - Om Mozilla
- MAC - Öppna ett Firefox fönster. Högst upp till vänster, klicka på Menyvalet Firefox - Om Mozilla Firefox.
- Linux - Öppna ett Firefox fönster. Klicka på Hjälp - Om Mozilla

- ▶ skadlig kod på nätet
- ▶ javascript
- ▶ flash
- ▶ java
- ▶ laddar ner pdf med skadlig kod
- ▶ laddar ner bild med skadlig kod

attackvektorer

- ▶ uppdatera program
- ▶ svartlista ej godkända program
- ▶ brandväggar

skydd igår

Warning - visiting this web site may harm your computer!


Suggestions:

- [Return to the previous page](#) and pick another result.
- Try another search to find what you're looking for.

Or you can continue to <http://www.iphonedevsdk.com/> at your own risk. For detailed information about the problems we found, visit Google's [Safe Browsing diagnostic page](#) for this site.

For more information about how to protect yourself from harmful software online, you can visit StopBadware.org.

If you are the owner of this web site, you can request a review of your site using Google's [Webmaster Tools](#). More information about the review process is available in Google's [Webmaster Help Center](#).

Advisory provided by 

► sandlådetekniker

skydd idag

ROMAB
Robert Malmgren AB

- ▶ sandbox
- ▶ app armor
- ▶ selinux
- ▶ jails
- ▶ chroot
- ▶ zoner
- ▶ virtualisering

sandlådetekniker

▶ selinux

- ◆ fedora

- ◆ redhat

- ◆ selinux sandbox

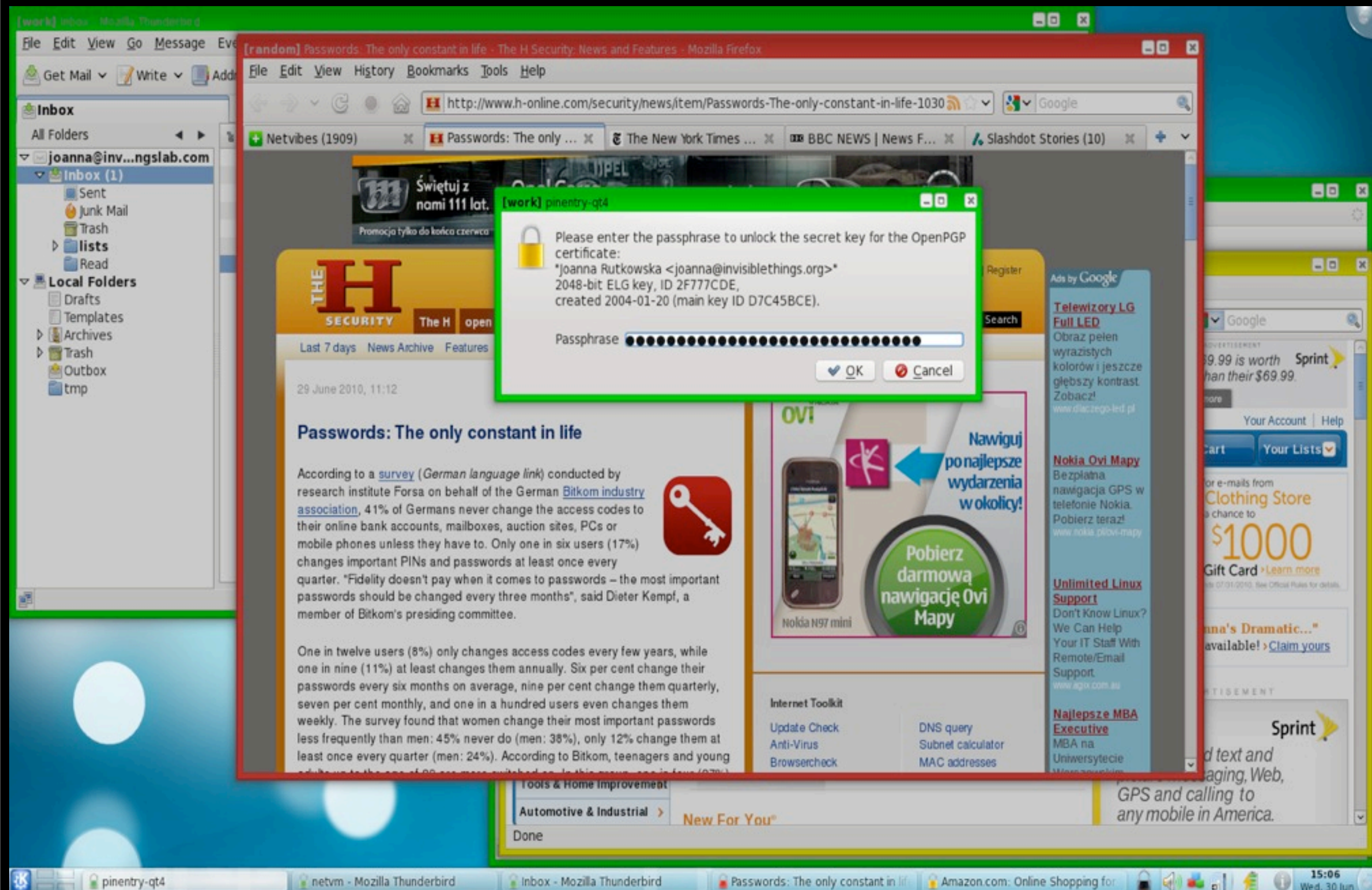
▶ apparmor

- ◆ ubuntu

▶ virtualisering

- ◆ cubes

sandbox linux



sandbox linux

ROMAB
Robert Malmgren AB

- ▶ Lyser med sin frånvaro, endast 2 skrivbordsprogram
- ▶ google chrome
- ▶ adobe reader X (google sandbox)
- ▶ negativa dac:lar
- ▶ vista+ använder även “integrity protection” (bantad biba)

sandbox windows

- ▶ ios kräver sandboxing
- ▶ mac osx har möjlighet till sandboxing sedan 10.5
- ▶ mac osx har sandboxing som användarvänligt tillval via xcode
- ▶ app store kräver sandboxing 1 mars 2012

sandbox apple

2011-11-15 07:00 MacWorld

Sandlådan i OS X inte säker

Av | **MacWorld**

Snart kommer Apple kräva att appar i Mac App Store använder OS X:s så kallade sandlåda, men denna har nu visat sig vara lätt att kringgå.



sandbox osäkert

ROMAB
Robert Malmgren AB

► förutsätter att program använder hemkatalogen

► få val

The screenshot shows the 'Entitlements' editor in Xcode. It is divided into two main sections: 'Entitlements' and 'App Sandbox'.

Entitlements Section:

- Enable Entitlements:** Checked (checkbox).
- Entitlements File:** A dropdown menu showing 'IronSettings'.
- iCloud Key-Value Store:** A text field containing 'com.romab.IronSettings'.
- iCloud Containers:** A list view containing 'com.romab.IronSettings'.

App Sandbox Section:

- Enable App Sandboxing:** Checked (checkbox).
- File System:** A dropdown menu showing 'None'. Below it are three unchecked checkboxes: 'Allow Downloads Folder Access', 'Allow Incoming Network Connections', and 'Allow Outgoing Network Connections'.
- Hardware:** Three unchecked checkboxes: 'Allow Camera Access', 'Allow Microphone Access', and 'Allow USB Access'. Below them are two more unchecked checkboxes: 'Allow Printing'.
- Apps:** Three unchecked checkboxes: 'Allow Address Book Data Access', 'Allow Location Services Access', and 'Allow Calendar Data Access'.
- Music Folder Access:** A dropdown menu showing 'Read Access'.
- Movies Folder Access:** A dropdown menu showing 'Read/Write Access'.
- Pictures Folder Access:** A dropdown menu showing 'None'.

sandbox i xcode

► mindre granularitet

```
(if (entitlement "com.apple.security.network.server")  
    (allow network-inbound (local ip)))
```

```
(allow network-inbound  
    (local tcp "*:88")  
    (local udp "*:88"))
```

sandbox i xcode

- ▶ fåtal program
- ▶ safari och quicktime sandboxar parsing av data
- ▶ iphoto sandboxar phototstream
- ▶ många temporära fixar

;;; Temporary fixes

;; <rdar://problem/9261425>, <rdar://problem/9376170>

(allow file-read* file-write*

(mount-relative-regex #"^/.Trashes(/|\$)"))

(home-subpath "/.Trash"))

apples sandbox

ROMAB
Robert Malmgren AB

- ▶ använder osx seatbelt/sandbox
- ▶ använder INTE entitlements
 - ◆ otillräcklig granularitet
 - ◆ otillräcklig determinism
- ▶ Cocoa launcher som startar perl för att bygga sandboxen
 - ◆ opensource :-)
 - ◆ gratis :-)
 - ◆ Fortfarande mindre usability-buggar. :-/

sandboxd[2320] ([95 | 24]): firefox-bin(95 | 24) deny mach-lookup
com.apple.CFPasteboardClient

sandboxd[1361] ([95 | 24]): firefox-bin(95 | 24) deny mach-lookup
com.apple.quicklook.ui.helper

sandboxd[98737] ([95 | 24]): firefox-bin(95 | 24) deny file-read-data /
Users/andreas/Library/
Preferences/.GlobalPreferences.plist.lockfile

sandboxd[98737] ([95 | 24]): firefox-bin(95 | 24) deny file-write-
unlink /Users/andreas/Library/Preferences/.GlobalPreferences.plist

sandboxd[98740] ([95 | 24]): firefox-bin(95 | 24) deny file-read-data /
Library/Preferences/SystemConfiguration/preferences.plist

sandboxd[98742] ([95 | 24]): firefox-bin(95 | 24) deny file-read-data /
Library/Preferences/SystemConfiguration/preferences.plist

sandboxd[98743] ([95 | 24]): firefox-bin(95 | 24) deny file-read-
metadata /Users/andreas/Documents

sandboxd[98743] ([95 | 24]): firefox-bin(95 | 24) deny file-read-
metadata /Volumes/NO NAME

F ■ å g o r ?