Tecnologia de identidade digital e criptografia no mundo *paperless*

Sergio Leal

CRYPTO ID

www.cryptoid.com.br

maior portal de notícias sobre certificação digital

ECMshow 2015

INFORMATION LEADERS FORUM

- ✓ Colunista e membro do conselho editorial do CryptoID.
- ✓ Especialista em Certificação Digital e Arquitetura Corporativa
- ✓ Trabalha com criptografia e certificação Digital desde o início da década de 90, tendo ocupado posições de destaque em empresas lideres em seu segmento como Modulo e CertiSign.
- ✓ Criador da ‘ittru': Primeira solução de certificação digital mobile no mundo.
- ✓ Bacharel em Ciências da Computação pela UERJ desde 1997.
- ✓ Certificações:
- ✓ Project Management Professional (desde 2007)
- ✓ TOGAF 9.1 Certified

ECMshow 2015
INFORMATION LEADERS FORUM


Paperless?
Digital
Disruption

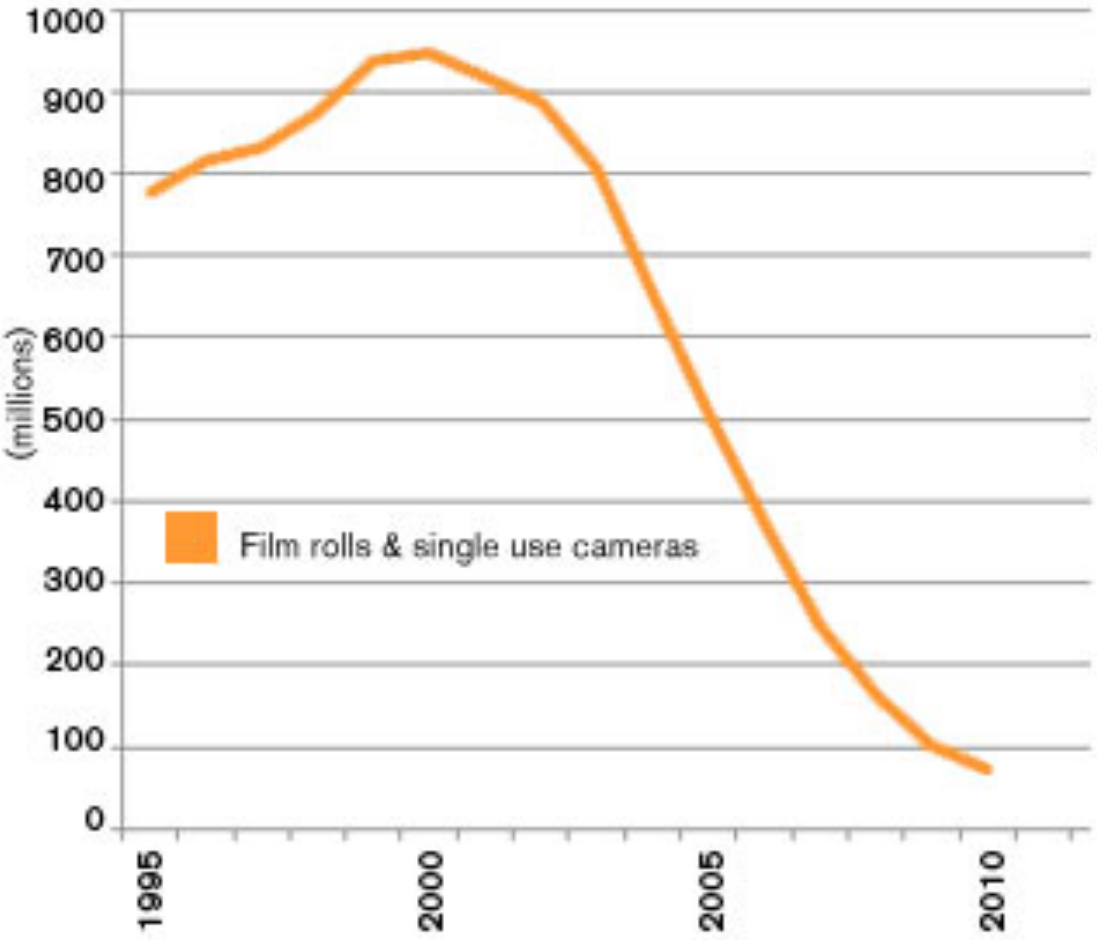
1975
Filmes 90%
Câmeras
85%

1975
Invenção da
Câmera
Digital

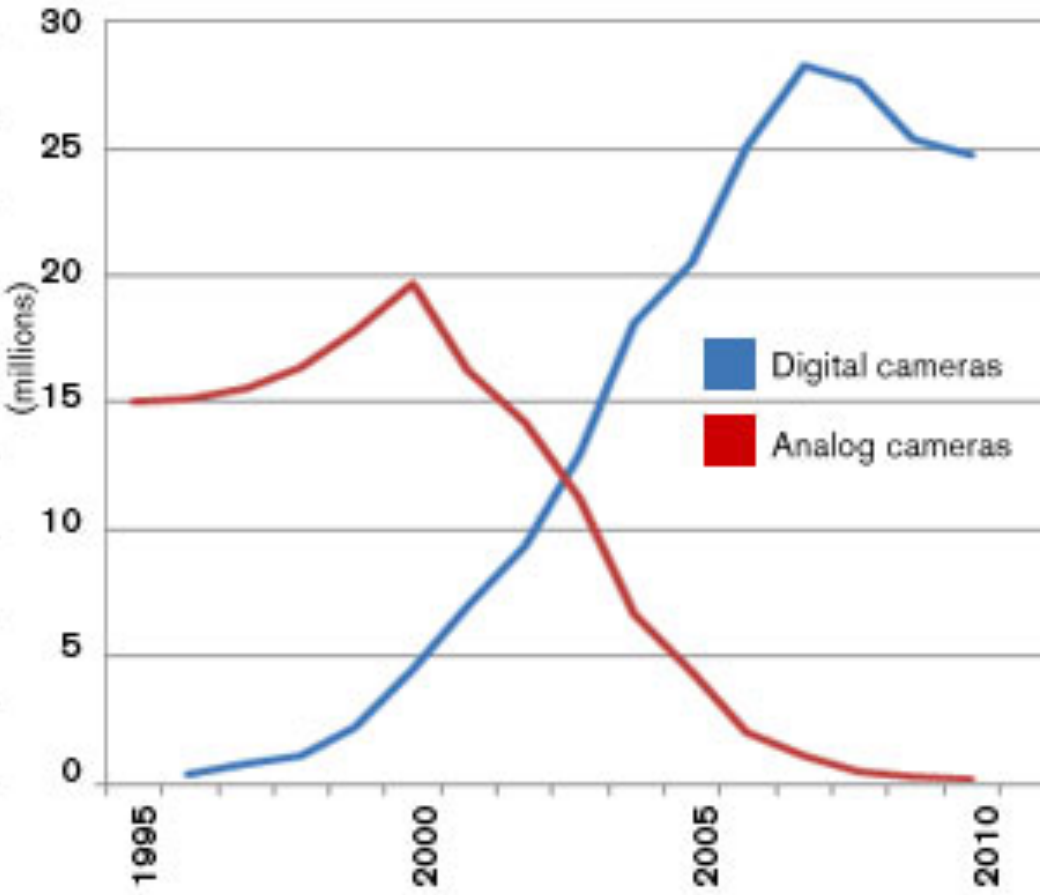
Fonte Wikipedia

Decline of Film

Film rolls sold



Camera sales



http://www.technologyreview.com/sites/default/files/legacy/kodak_charts_ab_x616.jpg

http://blog.softwareinsider.org/2014/02/18/research-summary-sneak-peaks-from-constellations-futurist-framework-and-2014-outlook-on-digital-disruption/screen-shot-2014-02-17-at-6-36-58-pm/

"Você pode ignorar a realidade, mas não pode ignorar as consequências de ignorar a realidade"

Ayn Rand

- ✓ *Contexto*
  - ✓ *Empresas e Serviços*
  - ✓ *Pessoas*
- ✓ *Identidade Digital*
- ✓ *Sigilo*
- ✓ *Conclusões*

UBER

airbnb

WhatsApp

NETFLIX

“Software vai devorar o mundo”

Marc Andreessen

WIRED

After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix

BUSINESS | DESIGN | ENTERTAINMENT | GEAR | SCIENCE

SHARE

SHARE 16368

TWEET 1473

PIN

ANDY GREENBERG SECURITY 07.24.15 12:30 PM

AFTER JEEP HACK, CHRYSLER RECALLS 1.4M VEHICLES FOR BUG FIX

Após hack de Jeep, Chrysler faz Recall

De 1,4 milhões de veículos

para consertar bug

ECMshow 2015

INFORMATION LEADERS FORUM

http://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/

Lucro da GM cai 88% no 1º tri após custos com recall em massa

COMENTE

Do UOL, em São Paulo 24/04/2014 | 12h52

Ouvir texto Imprimir Comunicar erro

A General Motors informou nesta quinta-feira (24) que o seu lucro no primeiro trimestre caiu 88% após um recall em massa, devido a defeito na chave de ignição de veículos.

Mas os resultados ainda superaram as expectativas em função das vendas de picapes da montadora na América do Norte.

O lucro líquido da GM no primeiro trimestre caiu para US$ 108 milhões, ou US$ 0,06 por ação, ante US$ 873 milhões, ou US$ 0,58 dólar, no mesmo período do ano passado. O trimestre mais recente incluiu custos de recall de US$ 0,48 por papel.

A receita subiu 1,4% na comparação anual, para US$ 37,4 bilhões, mas abaixo dos US$ 38,4 bilhões estimados por analistas.

O recall de milhões de veículos teve custo de US$ 1,3 bilhão e o defeito foi associado a 13 mortes. Defensores da segurança e alguns legisladores pediram que a GM estabelecesse um fundo de compensação para as vítimas.

ECMshow 2015
INFORMATION LEADERS FORUM

http://economia.uol.com.br/noticias/redacao/2014/04/24/lucro-da-gm-cai-88-no-1-tri-apos-custos-de-us-13-bi-com-recall-em-massa.htm

SHARE

SHARE 1817

TWEET 1160

PIN

COMMENT 142

KIM ZETTER SECURITY 08.06.15 6:00 AM

RESEARCHERS HACKED A MODEL S, BUT TESLA'S ALREADY RELEASED A PATCH

Pesquisadores hackearam um modelo S

mas Tesla já publicou um patch

http://www.wired.com/2015/08/researchers-hacked-model-s-teslas-already/

The Tesla Model S demolishes Consumer Reports' rating system

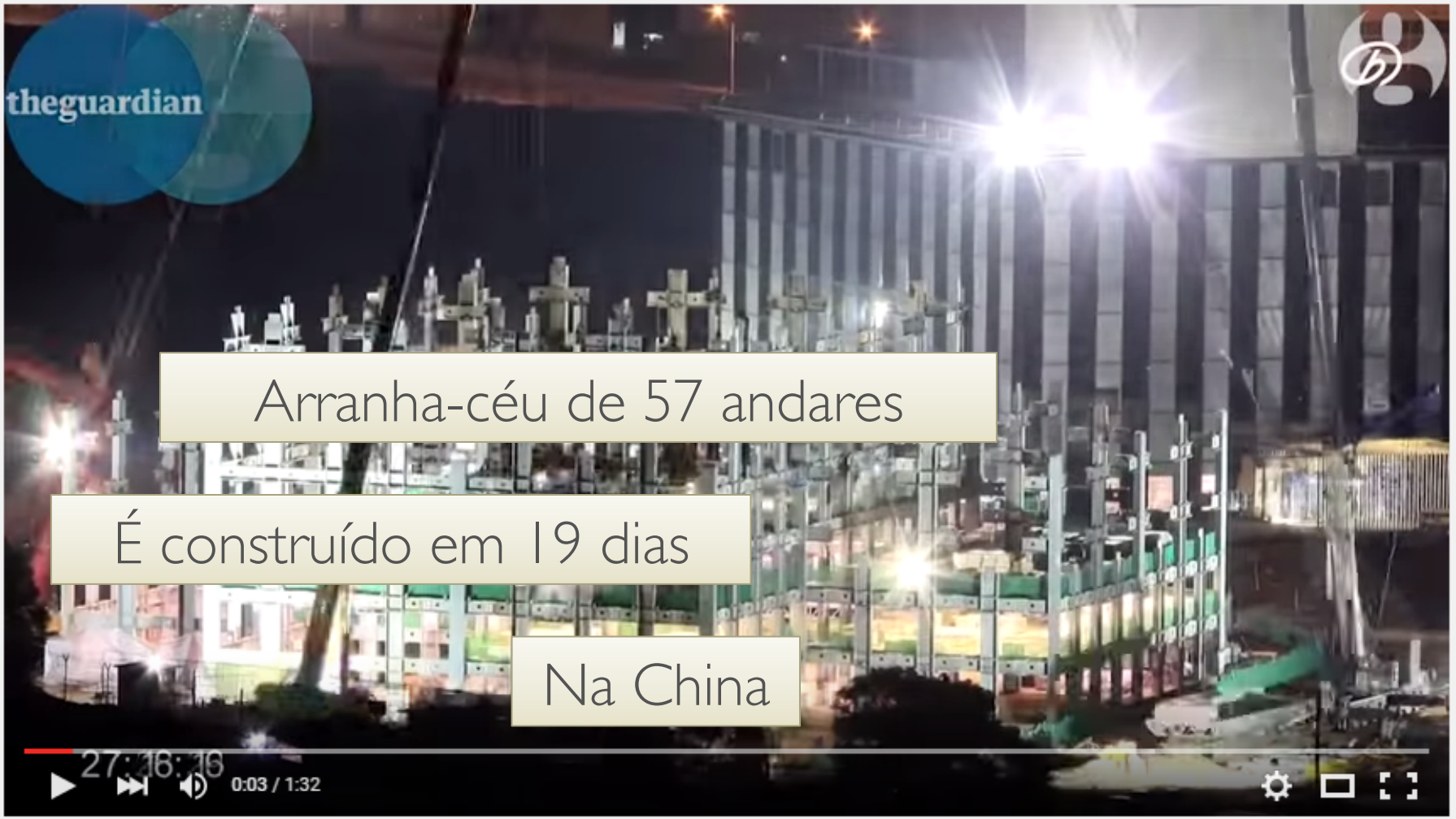
By Bill Howard on August 28, 2015 at 8:24 am | 111 Comments

Modelo S da Tesla demole

o sistema de notas

da *Consumer Reports*

http://www.extremetech.com/extreme/213066-grade-inflation-consumer-reports-rates-tesla-model-s-103-on-a-scale-of-100



Chinese build 57-storey skyscraper in 19 days – timelapse

https://www.youtube.com/watch?v=AhLk7L1B_fE

Geração	1940	1950	1960	1970	1980	1990	2000	2010
Baby Boomers								
Geração X								

Gerações Analógicas

Geração	1940				1980	1990	2000	2010
Baby Boomers								
Geração X								
Geração Y								

Geração Internet

Geração	1940	1950	1960	1970	1980	1990	2000	2010
Baby Boomers								
Geração X								
Geração Y								
Geração Z								

Geração Mobile / YouTube

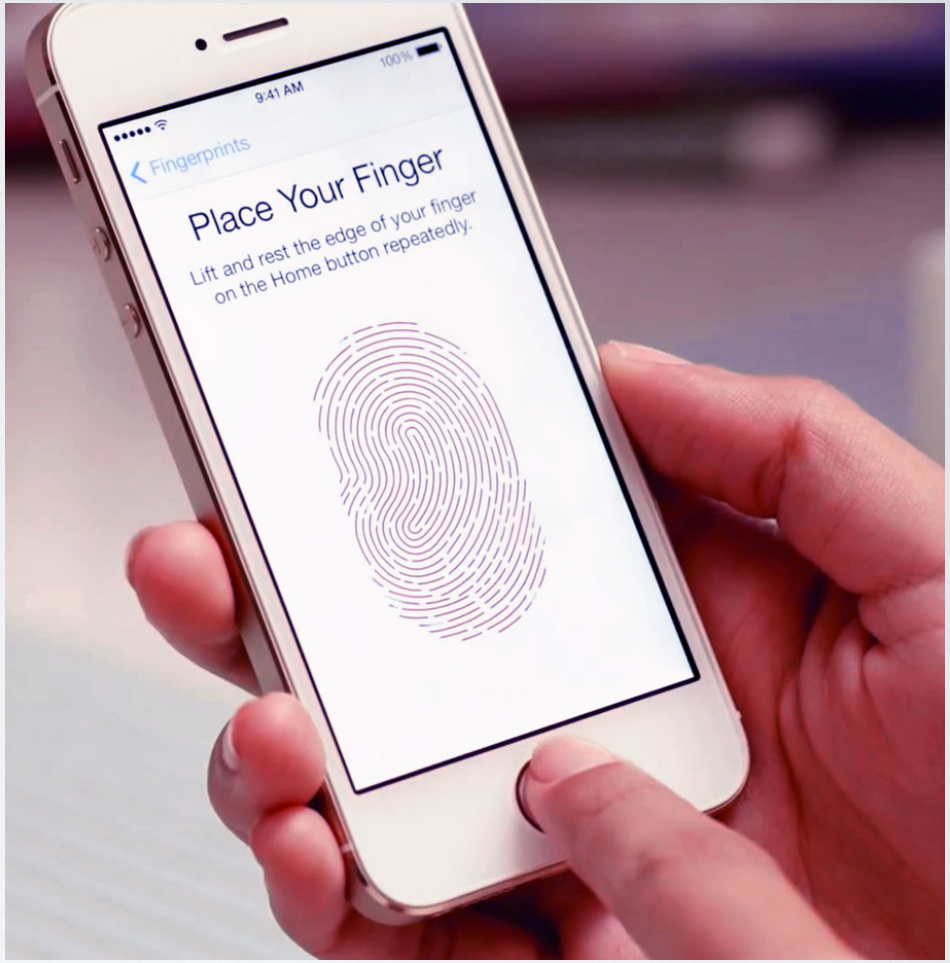
Identidade Digital

A compreensão humana

Senhas descatáveis

Credenciais para multiplos serviços

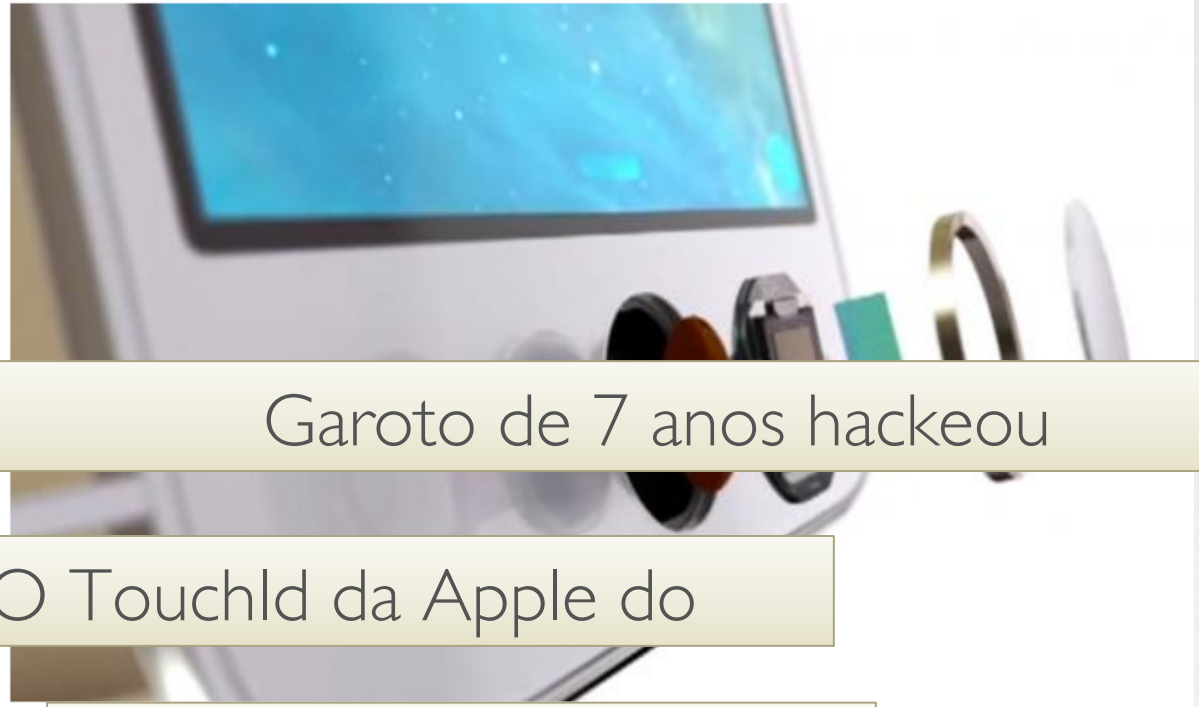
Biometria


9:41 AM
100%
Fingerprints
Place Your Finger
Lift and rest the edge of your finger on the Home button repeatedly.

Biometria

This 7-Year-Old Hacked Apple's Touch ID In The Simplest Way

NEWS | James Peckham | 13:26, 3 Dec 2014



Garoto de 7 anos hackeou

O TouchId da Apple do

A ne fingerprint se

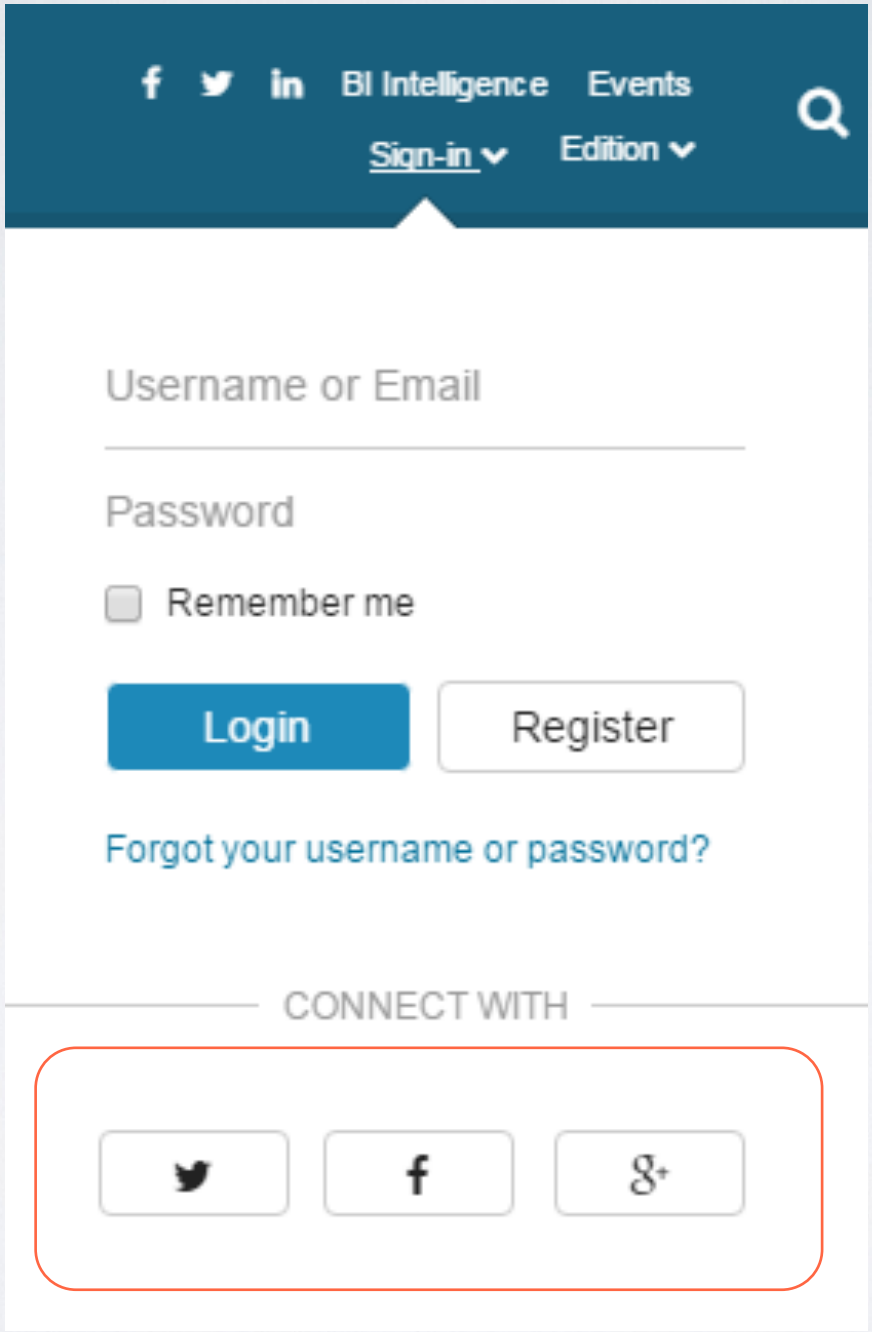
jeito mais simples

ECMshow 2015
INFORMATION LEADERS FORUM

Biometria

- ✓ Não permite múltiplas identidades;
- ✓ Independe da vontade;
- ✓ Não pode ser alterada;
- ✓ Sensores podem ser caros;

Autenticação Federada



Autenticação Federada

- ✓ Rastreamento de atividades

Internet das Coisas

Segurança em camadas

Hackers da Sony atacaram funcionários

com e-mails falsos de Apple ID

http://www.computerworld.com/article/2913805/cybercrime-hacking/sony-hackers-targeted-employees-with-fake-apple-id-emails.html

Como se sente?

Certificação Digital

- ✓ Não depende da compreensão humana;
- ✓ Permite operar "n para n";
- ✓ Permite múltiplas identidades;
- ✓ Não pode ser usado 'dormindo';
- ✓ Pode ser alterada;
- ✓ Não pode ser rastreado;

Validade Jurídica

Presidência da República
Casa Civil
Subchefia para Assuntos Jurídicos

MEDIDA PROVISÓRIA Nº 2.200-2, DE 24 DE AGOSTO DE 2001.

Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.

O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 62 da Constituição, adota a seguinte Medida Provisória, com força de lei:

Art. 1º Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

Art. 2º A ICP-Brasil, cuja organização será definida em regulamento, será composta por uma autoridade gestora de políticas e pela cadeia de autoridades certificadoras composta pela Autoridade Certificadora Raiz - AC Raiz, pelas Autoridades Certificadoras - AC e pelas Autoridades de Registro - AR.

Art. 3º A função de autoridade gestora de políticas será exercida pelo Comitê Gestor da ICP-Brasil, vinculado à Casa Civil da Presidência da República e composto por cinco representantes da sociedade civil, integrantes de setores interessados, designados pelo Presidente da República, e um representante de cada um dos seguintes órgãos, indicados por seus titulares:

I - Ministério da Justiça;

II - Ministério da Fazenda;

III - Ministério do Desenvolvimento, Indústria e Comércio Exterior;

IV - Ministério do Planejamento, Orçamento e Gestão;

V - Ministério da Ciência e Tecnologia;

VI - Casa Civil da Presidência da República; e

VII - Gabinete de Segurança Institucional da Presidência da República.

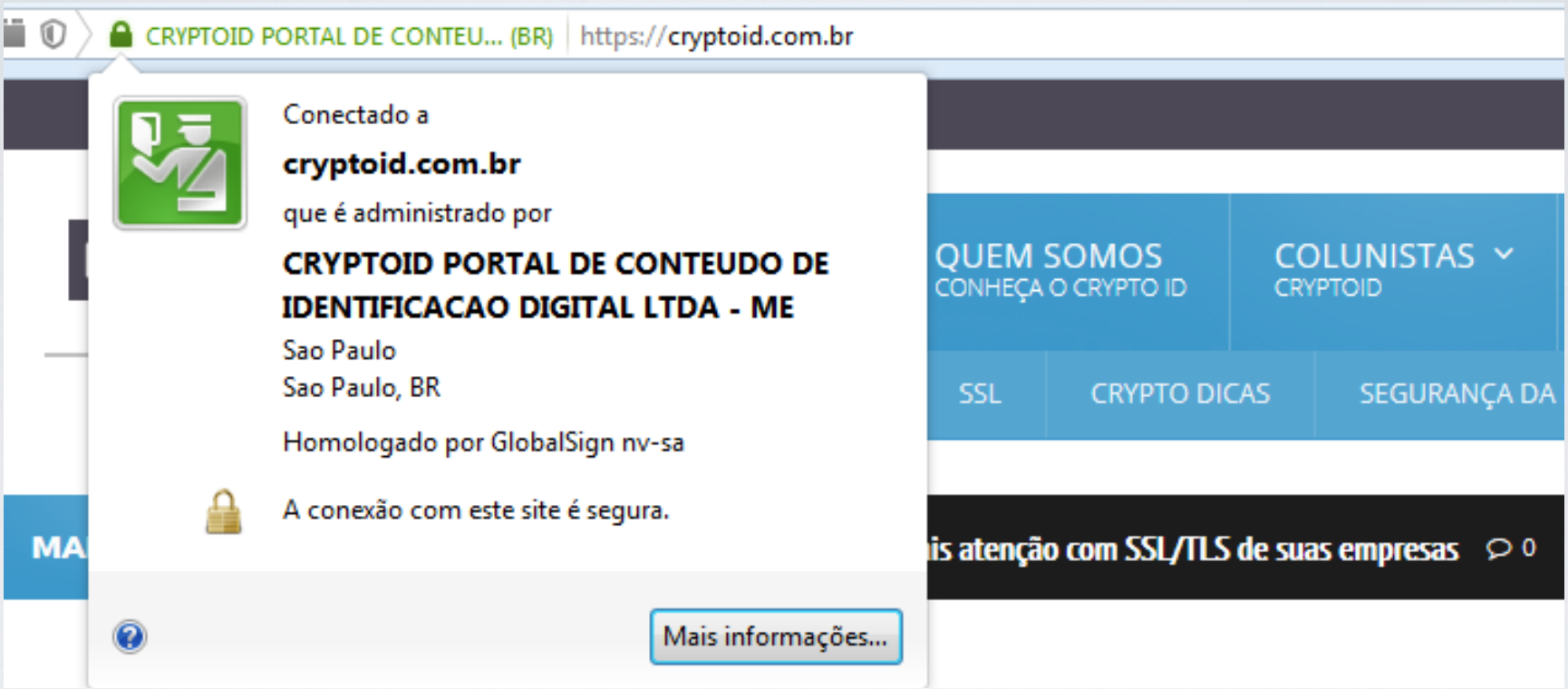
§ 1º A coordenação do Comitê Gestor da ICP-Brasil será exercida pelo representante da Casa Civil da Presidência da República.

§ 2º Os representantes da sociedade civil serão designados para períodos de dois anos, permitida a recondução.

§ 3º A participação no Comitê Gestor da ICP-Brasil é de relevante interesse público e não será remunerada.

http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-2.htm

O SSL/TLS é popular!



Quem tem?

ECMshow 2015
INFORMATION LEADERS FORUM


Aplicação
Applet Java
Active X
Java (JRE)
Navegador
MS-CAPI / PKCS#11 / MS-CGN
Sistema Operacional
13
PC/SC
Driver (USB)
USB
Driver (PC/SC)
Leitora
Driver (ISO7816)
Cartão


Aplicação
Applet Java
Active X
Java (JRE)
Navegador
MS-CAPI / PKCS#11 / MS-CGN
Sistema Operacional
PC/SC
Driver (USB)
USB
Driver (PC/SC)
Leitora
Driver (ISO7816)
Cartão


Aplicação
Applet Java
Active X
Java (JRE)
Navegador
MS-CAPI / PKCS#11 / MS-CGN
Sistema Operacional
PC/SC
Driver (USB)
USB
Driver (PC/SC)
Leitora
Driver (ISO7816)
Cartão


Aplicação
Applet Java
Active X
Java (JRE)
Navegador
MS-CAPI / PKCS#11 / MS-CGN
Sistema Operacional
PC/SC
Driver (USB)
USB
Driver (PC/SC)
Leitora
Driver (ISO7816)
Cartão


Aplicação
Applet Java
Active X
Java (JRE)
Navegador
MS-CAPI / PKCS#11 / MS-CGN
Sistema Operacional
PC/SC
Driver (USB)
USB
Driver (PC/SC)
Leitora
Driver (ISO7816)
Cartão


Aplicação
Applet Java
Active X
Java (JRE)
Navegador
MS-CAPI / PKCS#11 / MS-CGN
Sistema Operacional
PC/SC
Driver (USB)
USB
Driver (PC/SC)
Leitora
Driver (ISO7816)
Cartão


Aplicação
Applet Java
Active X
Java (JRE)
Navegador
MS-CAPI / PKCS#11 / MS-CGN
Sistema Operacional
PC/SC
Driver (USB)
USB
Driver (PC/SC)
Leitora
Driver (ISO7816)
Cartão


Aplicação
Applet Java
Active X
Java (JRE)
Navegador
MS-CAPI / PKCS#11 / MS-CGN
Sistema Operacional
PC/SC
Driver (USB)
USB
Driver (PC/SC)
Leitora
Driver (ISO7816)
Cartão


Aplicação
Applet Java
Active X
Java (JRE)
Navegador
MS-CAPI / PKCS#11 / MS-CGN
Sistema Operacional
PC/SC
Driver (USB)
USB
Driver (PC/SC)
Leitora
Driver (ISO7816)
Cartão


Aplicação
Applet Java
Active X
Java (JRE)
Navegador
MS-CAPI / PKCS#11 / MS-CGN
Sistema Operacional
PC/SC
Driver (USB)
USB
Driver (PC/SC)
Leitora
Driver (ISO7816)
Cartão

ittru

O GLOBO ☰ MENU | SOCIEDADE ▾ | COMPARTILHAR | BUSCAR | CLIQUE E ASSINE

Programa criado por cariocas simplifica acesso a certificados digitais

POR CARLOS ALBERTO TEIXEIRA / / /
21/02/2010 0:00 / ATUALIZADO 01/11/2011 21:00

Com a ajuda do telefone celular, o processo de certificação bolado pela Timewarp com o Ittru parece mais simples que os métodos tradicionais Crédito: AFP Photo -

ECMshow 2015
INFORMATION LEADERS FORUM

http://oglobo.globo.com/sociedade/tecnologia/programa-criado-por-cariocas-simplifica-acesso-certificados-digitais-3051035

ARQUIVO CRYPTO ID COLUNISTAS DESTAQUES SERGIO LEAL

Você conhece a Web Cryptography API da W3C?

http://oglobo.globo.com/sociedade/tecnologia/programa-criado-por-cariocas-simplifica-acesso-certificados-digitais-3051035

ARQUIVO CRYPTO ID CERTIFICAÇÃO DIGITAL DESTAQUES LEGISLAÇÃO, RECURSOS E NORMAS

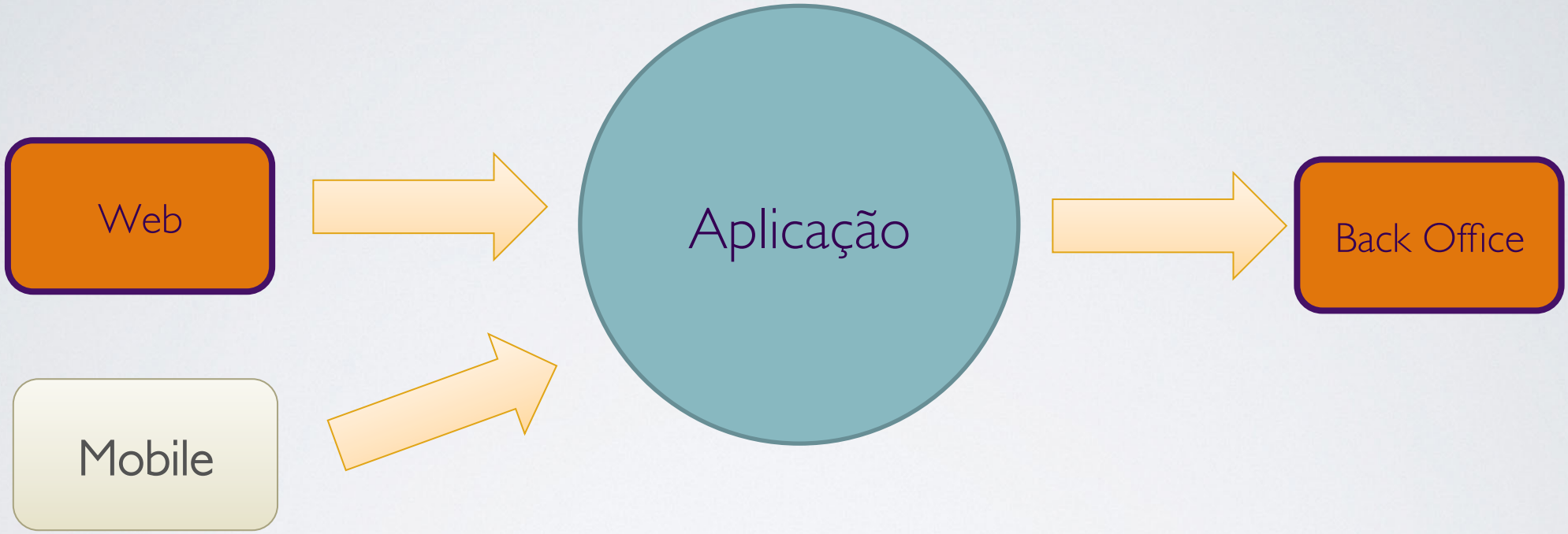
Hackers invadem Ibama e com certificado digital liberam venda de madeira

https://cryptoid.com.br/arquivo-cryptoid/hackers-invadem-ibama-e-com-certificado-digital-liberam-venda-de-madeira/

Como Começa?

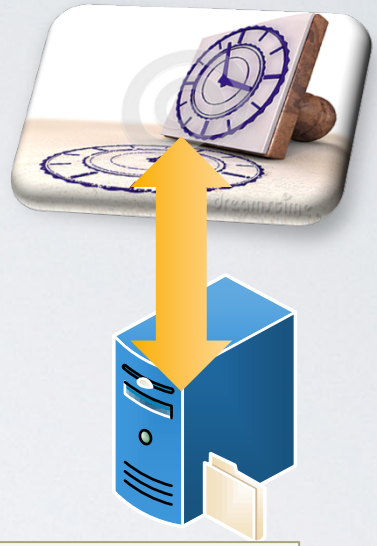
Arquitetura Web

+ Mobile



O que encontramos?

Como é?



SigningTime
Countersignature

CAdES
XAdES
PAdES
CMS
XMLDSig

Java

PKCS#11 MSCAPI PC/SC

Software Livre

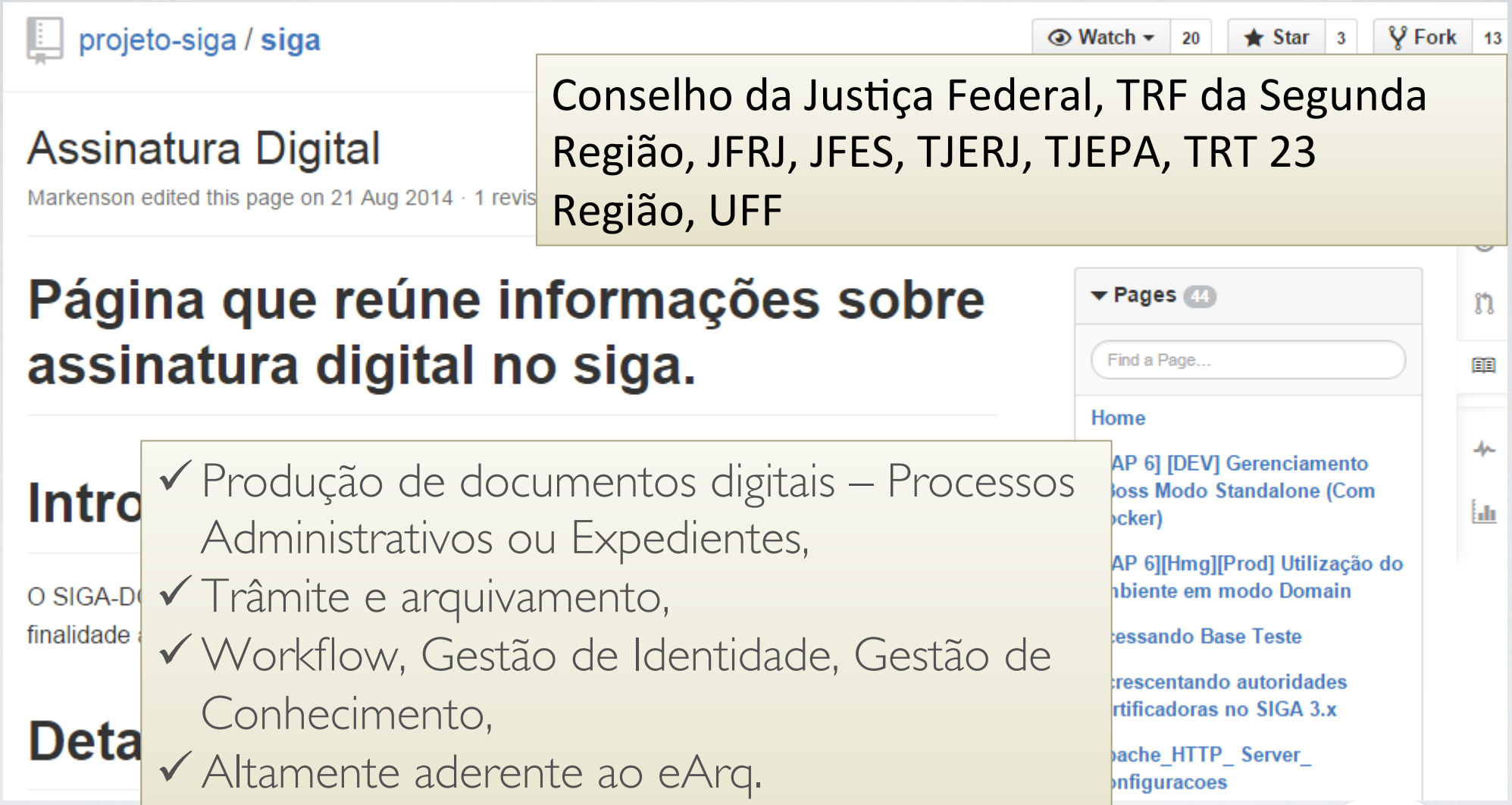
Software Livre para assinatura digital

- ✓ Segue padrões ICP-Brasil
- ✓ ADRB 1.0 e 2.1
- ✓ Orientado a serviço
- ✓ Multi browser, multi OS
- ✓ Substitui o CAPICOM
- ✓ Integrável a qualquer aplicativo web
- ✓ Java, .NET, PHP..
- ✓ Pode ser usado em aplicativos desktop
- ✓ Oferece ActvieX
- ✓ Applet (PKCS#11 e MSCAPI)

http://bluecryst.al

ECMshow 2015
INFORMATION LEADERS FORUM

Software Livre



Conselho da Justiça Federal, TRF da Segunda Região, JFRJ, JFES, TJERJ, TJEPA, TRT 23 Região, UFF

- ✓ Produção de documentos digitais – Processos Administrativos ou Expedientes,
- ✓ Trâmite e arquivamento,
- ✓ Workflow, Gestão de Identidade, Gestão de Conhecimento,
- ✓ Altamente aderente ao eArq.

https://github.com/projeto-siga/siga/wiki/Assinatura-Digital

E o Governo?

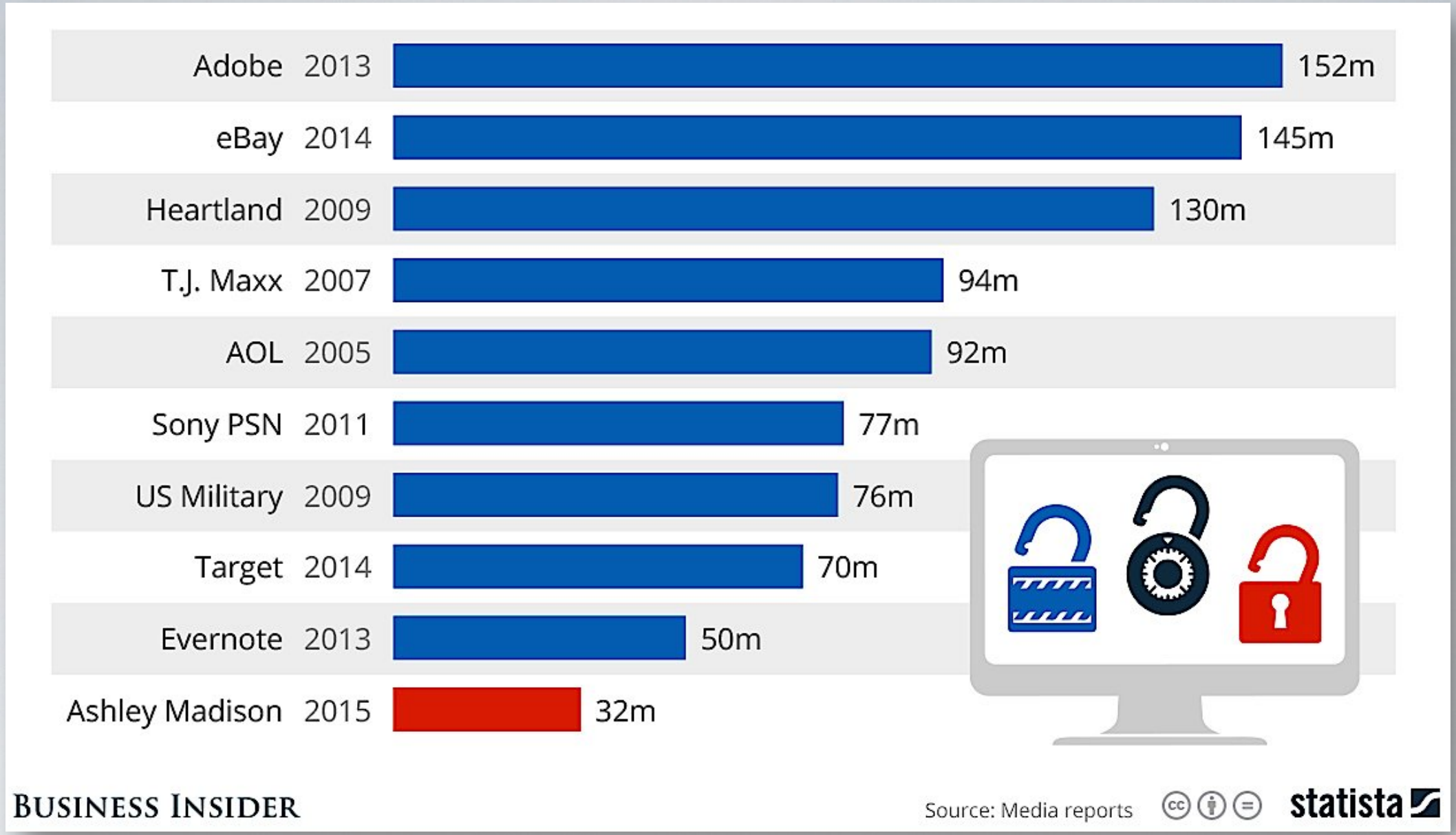
PJe supera marca dos 5 milhões de processos eletrônicos

25/08/2015 - 10h03

TWEETAR COMPARTILHAR

http://www.cnj.jus.br/noticias/cnj/80258-pje-supera-marca-dos-5-milhoes-de-processos-eletronicos

Sigilo



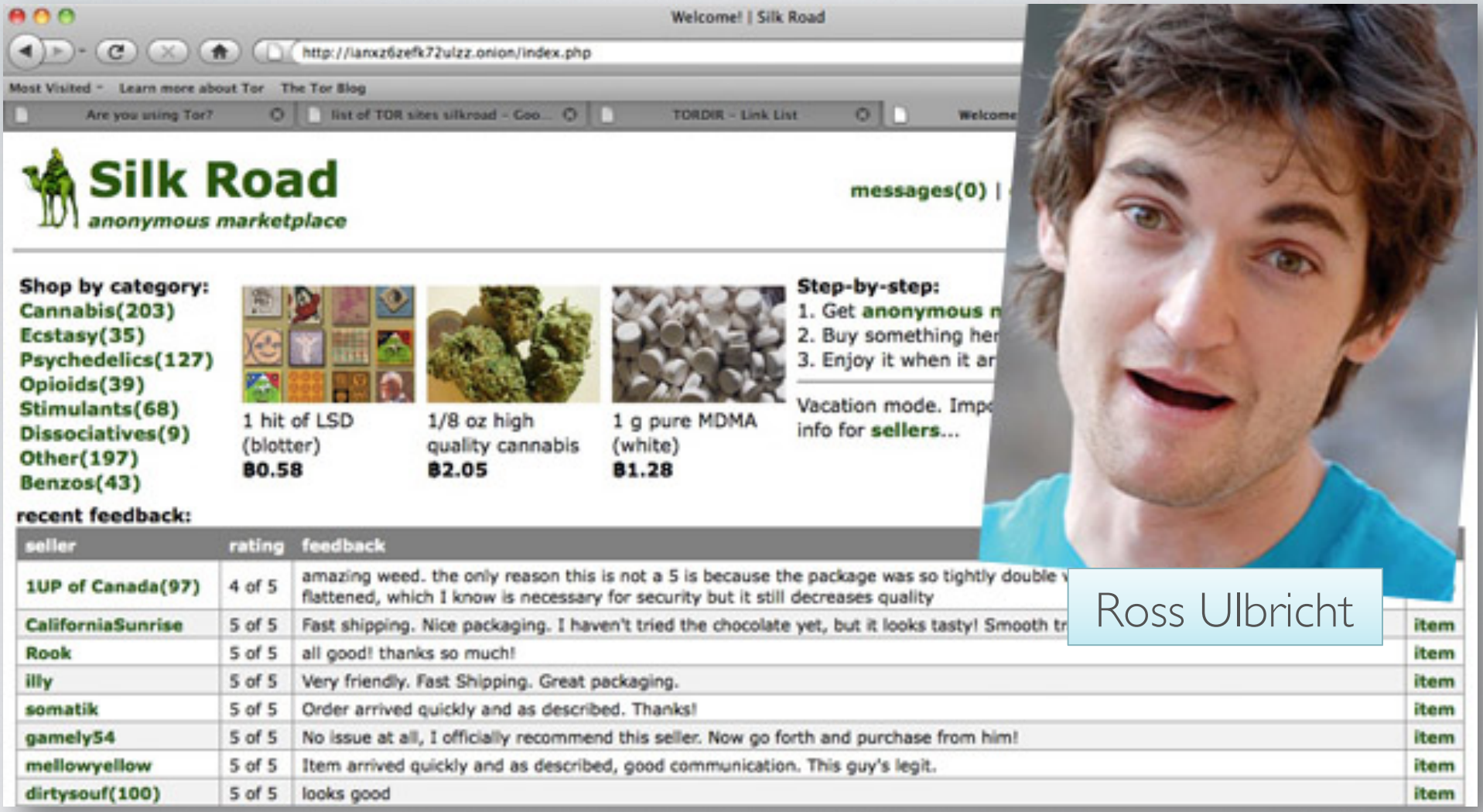
http://www.businessinsider.com/ashley-madison-hack-names-stolen-vs-other-hacks-2015-8

"*Criptografia é única solução* para escapar da espionagem"

Edward Snowden

ECMshow 2015
INFORMATION LEADERS FORUM

Nem os criminosos



Obrigado!

Sergio Leal (sergio.leal@ittru.com)

http://bluecryst.al