



NEVIS Forum 2019

Welcome





NEVIS Update: What happened in a year



Stephan Schweizer
CPO NEVIS



FIDO Alliance



FIDO Alliance:

- The FIDO (Fast IDentity Online) Alliance, fidoalliance.org was formed in July 2012 to address the lack of interoperability among strong authentication technologies

AdNovum Involvement

- Our Mobile Auth solution is based on FIDO
- We are sponsor member since April 2019
- FIDO certification for NEVIS is in process

KuppingerCole Leadership Compass




AdNovum continues to execute well on their roadmap by adding new features, such as the introduction of their FIDO UAF 1.1 support for their authentication server and mobile SDK for iOS and Android. Other improvements include deployment support with Ansible and Docker.

Security	strong positive
Functionality	strong positive
Integration	positive
Interoperability	strong positive
Usability	strong positive

Table 1: AdNovum rating

AdNovum's continued development to added new features and fill in missing gaps helps them to advance as a product leader.

Cure53 Security Assessment



Successful Cure53 Assessment
Penetration test and source code audit 2018

NEVIS emerges victorious from security assessment by Germany's penetration testing experts of Cure53

Cure53 tests NEVIS Security Suite

Given the complexity of the AdNovum NEVIS Security Suite, as well as the age of some of the sources, Cure53 was positively surprised in how well security has been managed in the tested compound. Based on the findings, the Cure53 team could only conclude that the AdNovum NEVIS Security Suite emerged victorious from this 2018 security assessment. The achieved outcomes – in terms of both the low number and limited severities of the findings – are rare and praiseworthy.

Read more and download the management summary provided by [cure53](#) below.

[...] It was also ascertained that the **sole** vulnerability spotted on the scope carried a “*Medium*” security ranking only. In other words, **no problems** that could be deemed as triggering “*Critical*” or even just “*High*”-ranking risks could be unveiled. [...]

Despite intensified efforts from the Cure53 team, **no major defects** like Remote Code Execution, privilege escalation or authentication bypasses could be found on the AdNovum scope.



Identity 4.0: Smart, sexy und trotzdem sicher?



Stephan Schweizer
CPO NEVIS



Challenge: Explain your IT job to an elder person...

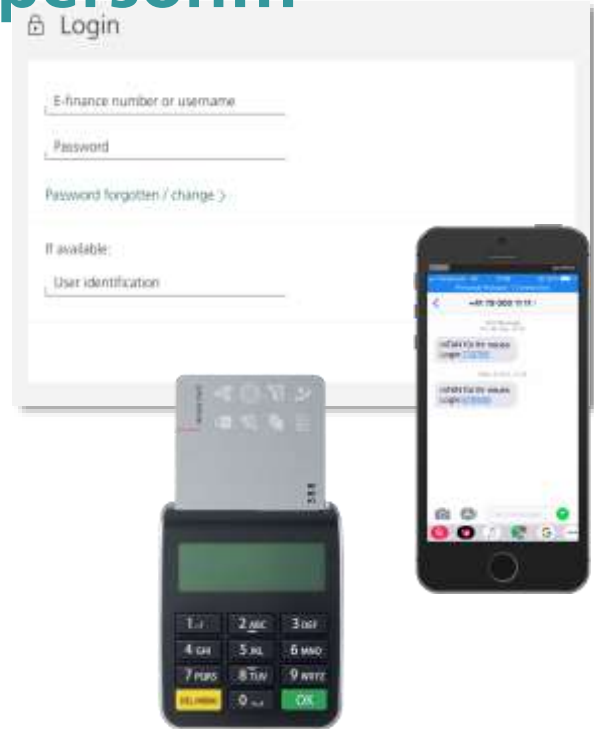
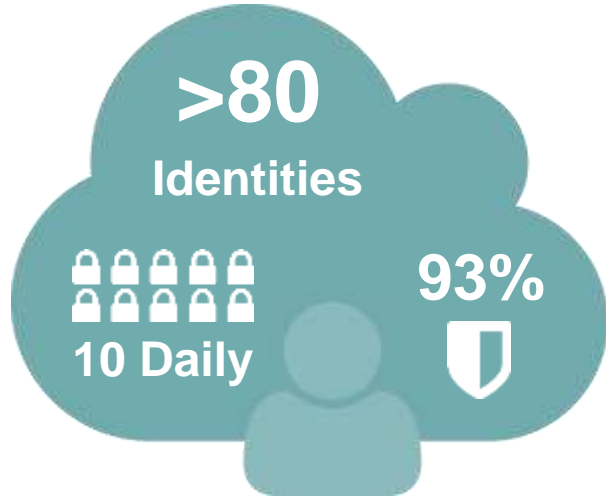


Image Source: Ivan Chiosea / Alamy Stock Foto

User perspective: Identity Silos

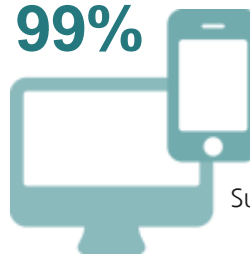


Growing user challenges

- 22% of users have > 80 identities (2016: 4%)
- 87% use up to 10 IDs on a daily basis (2016: 42%)
- 93% at least one account with 2FA (2016: 90%)

Multi-Channel is reality:

use their
accounts on
both
mobile and
pc

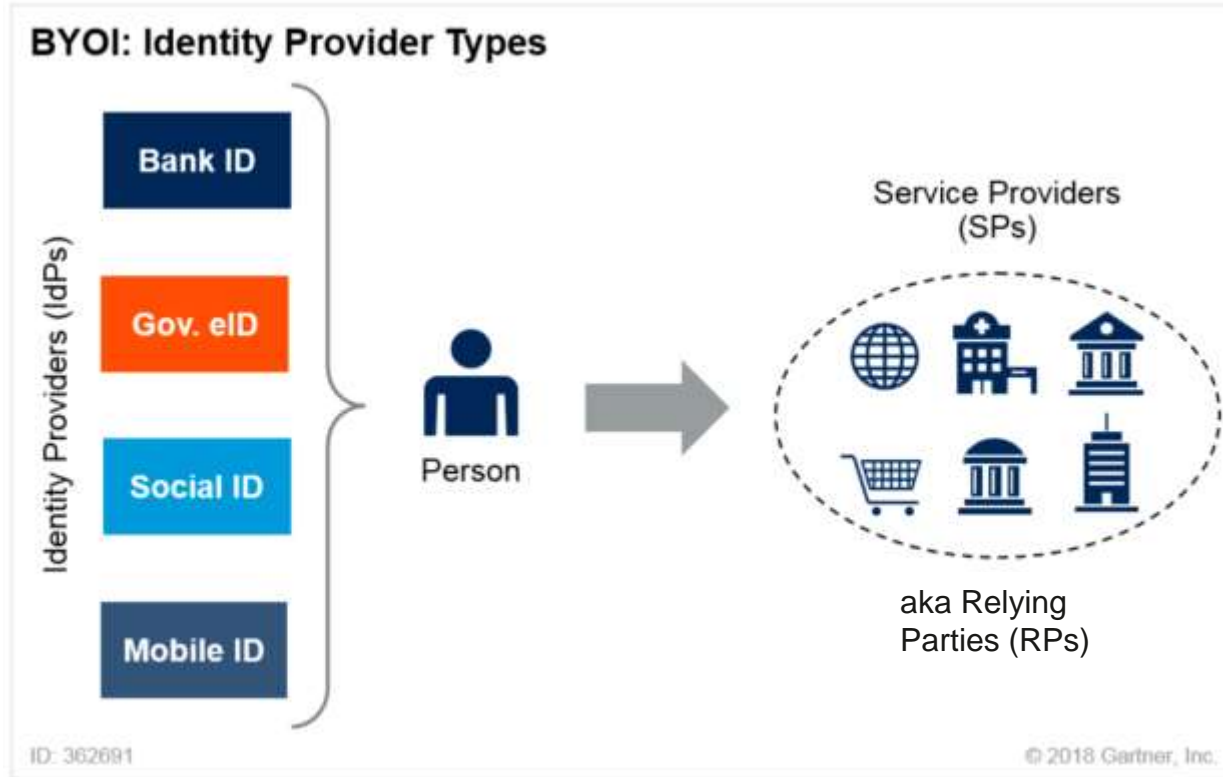


99%

Survey 2016: 93%

Source: AdNovum Digital Identities Survey, September 2018

BYOI (Bring Your Own Identity) ≠ Social Login



Pitfall: The NASCAR Problem



Paradox of Choice:
Negative Impact on User Experience

My Account

Login

Username or email address *

Password *

Remember me

[Lost your password?](#)

For faster checkout, login or register using your social account:

Register

Email address *

Password *

What are the big ones doing?

Twitter login and sign-up form. Fields for phone number, email address, and password. Includes a "Log In" button and a "Join Twitter today" section with "Sign Up" and "Log In" buttons.

Facebook account creation form. Fields for email or phone, password, first name, and surname. Includes a "Log In" button and a "Create an account" button.

Google sign-in form. Fields for email or phone. Includes a "Log In" button and a "Create account" button.

PayPal login and sign-up form. Fields for email address and password. Includes a "Log In" button and a "Sign Up" button.

Amazon sign-in form. Fields for email (phone for mobile accounts) and password. Includes a "Log In" button and a "Create your Amazon account" button.

Good reasons to become an Identity Provider



Business Model

Monetizing of identity data is part of the business model



Brand Loyalty

Strong brand, standing for trust is an ideal prerequisite to become an IDP



Security and Privacy Concerns

Available Identity Providers are not fulfilling the requirements



User Demographics

A part of your user base is not covered by an appropriate IDP

The challenge of every IDP: What about passwords?

The Man Who Wrote Those Password Rules Has a New Tip: N3v\$r M1-d!

Bill Burr's 2003 report recommended using numbers, obscure characters and capital letters and updating regularly—he regrets the error



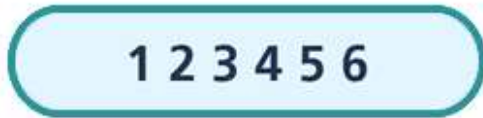
Advice on passwords is changing. PHOTO: MOMENT EDITORIAL/GETTY IMAGES



- Bad user habits
- For machines, these Passwords are easy to guess

Source: <https://www.wsj.com/articles/the-man-who-wrote-those-password-rules-has-a-new-tip-n3v-r-m1-d-1502124118>

Bad password habits



85%

Are too lazy to change password often



33%

Re-use password for most accounts



40%

Cannot login because of missing token or card reader

Source: AdNovum Digital Identities Survey, September 2018

User habits are even worse on Mobile

- Passwords created on smartphones are significantly shorter than on PCs
- Significantly fewer upper case letters
- No use of symbols by **25.1% of users on PCs**
- No use of symbols by **43.8% of users on Mobile**



Source: Emanuel von Zezschwitz, Alexander De Luca, and Heinrich Hussmann. 2014. Honey, I shrunk the keys ...

Identity theft: Still big business

Account Type	Price Range
 Retail: Major retailers, fashion, entertainment, home goods, auto	\$0.20 - \$6.00
 Social: Social media, emails, dating sites, instant messaging	\$1.00 - \$10.00
 Hospitality: Airlines, hotels, and travel	\$0.70 - \$10.50
 Financial: Bank accounts, money transfer services, credit cards	\$0.50 - \$15.50
 Technology: Telecommunications, mobile devices and electronics, business services	\$0.40 - \$4.50

Identity theft market:

- Globally, approx. **4.5 billion accounts** compromised in 1st half year 2018
- Prices depend on “freshness” of stolen identity data
- **Highly automated trading** by using “Telegram” messaging service

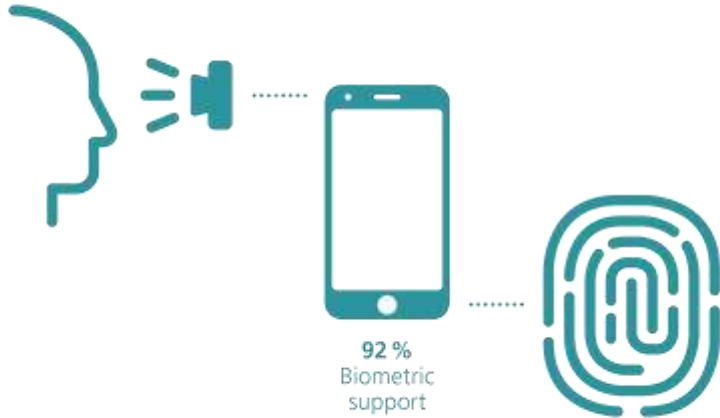


Source: RSA Quarterly Fraud Report, Q4 2018

Time to change: Our vision on passwords....

The good news: There is a way out!

Biometric support on devices



Rising popularity for biometric authentication



Source: AdNovum Digital Identities Survey, September 2018

Demo: Passwordless Login



What about compliance? (PSD2 = Payment Service Directive v2, EU legislation)

PSD2 Strong Customer Authentication (SCA, Chapter II)

- At least two of three elements:
 - Something you know (e.g. password)
 - Something you have (e.g. device)
 - Something you are (e.g. biometrics)
- The authentication of a user must result in a cryptographic signature
- The user's cryptographic material must be well protected

Transaction Confirmation / Dynamic Linking

- Cryptographic Authentication Code needs to be linked to Transaction



Perfectly fulfilled by passwordless login



And the user feedback?



Image Source: Ivan Chiosea / Alamy Stock Foto

Conclusion

**BYOID
mitigates the
ID explosion**

However, there will most probably never be a “magic single Identity Provider”

**Keep Users in
Mind**

Surprisingly, millennials and elderly people have very similar expectations!

**It's time to
retire
passwords**

The technology and standards are available now!



... since without user convenience there will be nothing left to be protected!



Thank you! Questions?