1. One-sentence description

Excalibur eliminates passwords, moving all your existing password-protected devices and systems seamlessly to smartphone-based multi-factor authentication utilizing contextual physical-security.

2. Brief project description

Excalibur utilizes the mobile phone as a secure hardware token for **any and all** authentication and authorization needs inside of the enterprise. It achieves the ultimate goal of moving all authentication and authorization away from passwords, replacing them seamlessly with smartphone-based strong but user friendly multi-factor authentication. Excalibur's unique value is in providing backward compatibility with all the applications, **Operating Systems (OS)** and services the enterprise uses today. Excalibur **bridges the password-based present day and password-free future, *massively improving security and making it super easy to use at the same time.***

3. Problem description

Once usage of any system reaches certain critical mass it becomes very hard to replace. Passwords are a prime example of such critical mass behavior – everybody understands passwords are not future proof, not practically secure and not user friendly, yet they are still at the core of practically every enterprise system used.

Instead of replacing the password, second factor authentication became the de-facto standard – it is obvious that it is just a quick fix not a real solution. Can't we do better?

Passwords are everywhere, any system that would try to directly replace them would fail on legacy compatibility. **Even the approach taken by Microsoft's Windows Hello for Business still uses passwords** – the user must still know their password, just the frequency how often it is necessary to type it is reduced. Yet, it is still there thus it still represents a security risk due to all possible attacks on passwords. Also, all the password management must still be in place etc. **The same is true for any enterprise Single Sign-on (SSO) solution such as Okta, Ping Identity, Duo…**

4. The Solution

The only way to eliminate passwords is to abstract them. Excalibur takes a completely novel and unique approach – it creates a **transparent password abstraction layer** – injecting randomly generated credentials into classic legacy authentication protocols / mechanisms. **The password is still there, it just doesn't hold any security value anymore** – it is randomly generated and never stored at a single location from where it could be stolen. **There is no single point of failure anymore – no central storage, no central control element. No possibility to leak anything useful or impersonate.** To achieve these unique properties Excalibur uses a **fully distributed cryptographical scheme for both storage and control logic** backed by HW PKI / HSM and integrates natively into not only the host Operating System (OS) but also into the central authentication system of an enterprise which is usually the Active Directory (AD).

From the perspective of the user - **authentication is instantly completely password-free.** The user only interacts with his / her smartphone – using it to provide authentication factors such as phone-based biometry, cloud-based biometry (**utilizing Microsoft Azure Cognitive Services**), geolocation, proximity to other devices, peer verification, PIN code if no phone biometry is present and of course phone ownership is also a factor. **All these factors are combined** into a simple and **straightforward user experience** where the user **can't do anything wrong** but also **can't delegate access in any way.**

At the same time **complete compatibility** with all the password-based systems is achieved. All attacks on credentials are defeated because the password is no longer static – instead it is a **constantly changing random** string that cannot be reused and the user doesn't even know it. No more phishing, credential stealing malware, keyloggers or even attacks on Kerberos which is the most popular attack vector for lateral movement after initial system compromise.

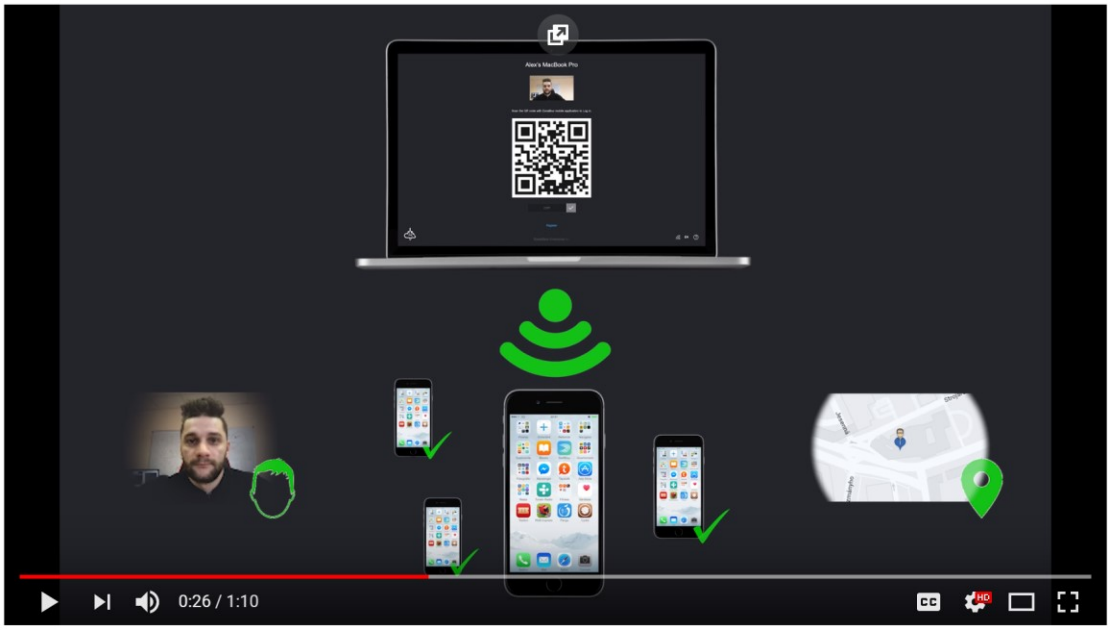
Contact: Ing. Ivan Klimek, PhD., CEO/CTO/Founder
mailto: ivan@xclbr.com
https://linkedin.com/in/ivanklimek

5. Short Demo

Windows Login couldn't be simpler! (domain / local account) - https://youtu.be/u8HdARm3Ejw

In the worst case - **if phone has no HW biometric sensor** - the PIN code + front facing camera face recognition, location and phone ownership factor will be used.

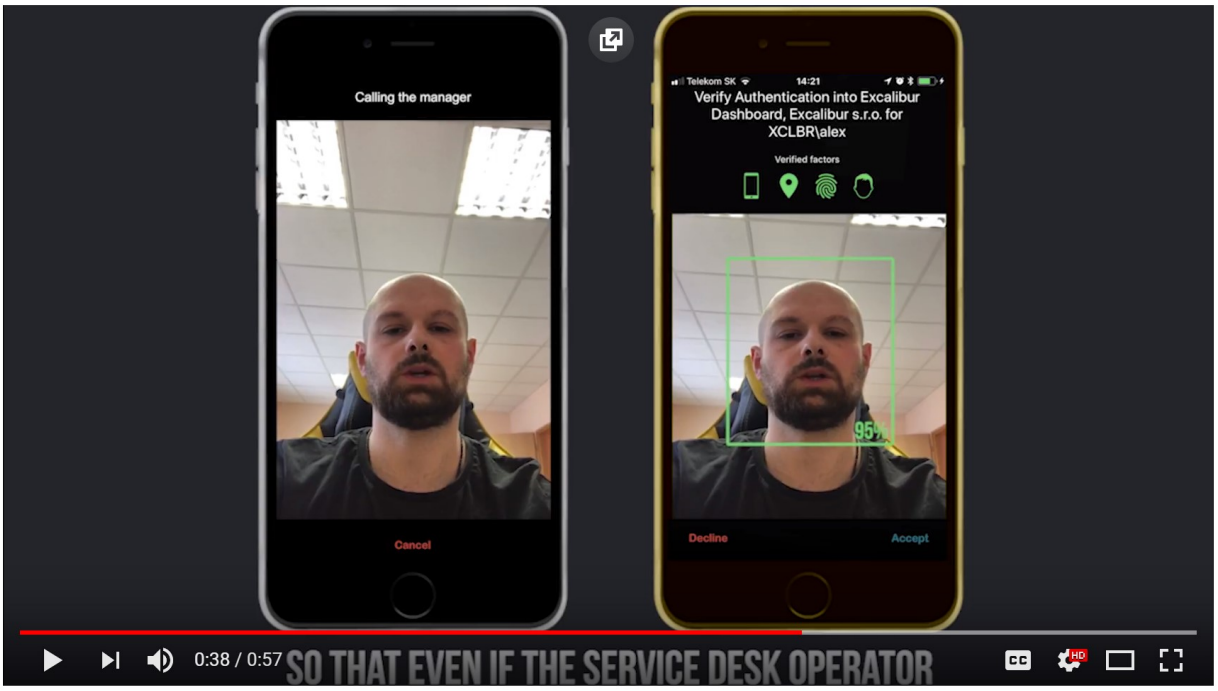
Dynamically generated QR code is used because it always works – not all devices have Bluetooth, for example thin clients. **If Bluetooth or other utilizable technologies such as front facing camera on the PC are present,** they can be used to improve the user experience as the next video demonstrates on mac OS: https://youtu.be/jzQdX71rUSw



Contact: Ing. Ivan Klimek, PhD., CEO/CTO/Founder
mailto: ivan@xclbr.com
https://linkedin.com/in/ivanklimek

6. Uniqueness

All other Enterprise Identity Management platforms are password based, removing the password opens completely novel possibilities. For example, with Excalibur it is possible for **users to vouch for each other** – this allows to use existing organizational structure (present in the AD) to bootstrap a direct trust structure – who is reporting to whom. Utilizing this information instantly enables any **Manager to confirm the identity** of his / her subordinates for example when they initialize a new phone, or a security policy blocks their access. **Moving security to the "physical layer"** – either via direct physical verification or utilizing build-in video call with embedded face recognition. This allows most security incidents to be resolved where they happen – at the branch office - without the need to escalate to security operations center, **saving resources but also enabling a much more flexible and strict security posture**. Why strict? Because utilizing this approach the system has both negative and positive feedback – if it creates a policy too strict – the user will be blocked and needs to be allowed by a peer – this is a clear negative signal, if policy is automatically made stricter but "nobody complains" this is a positive signal. *This way Excalibur machine-learns and automatically applies the strictest possible security policy individualized for each user, and at the same time is adaptable to any changes (relocation / business trip / …) without any Administrative interaction necessary.* **There is no other password-less, self-improving identity platform, compatible with existing enterprise systems!**



https://youtu.be/TfzDzMPNOHU

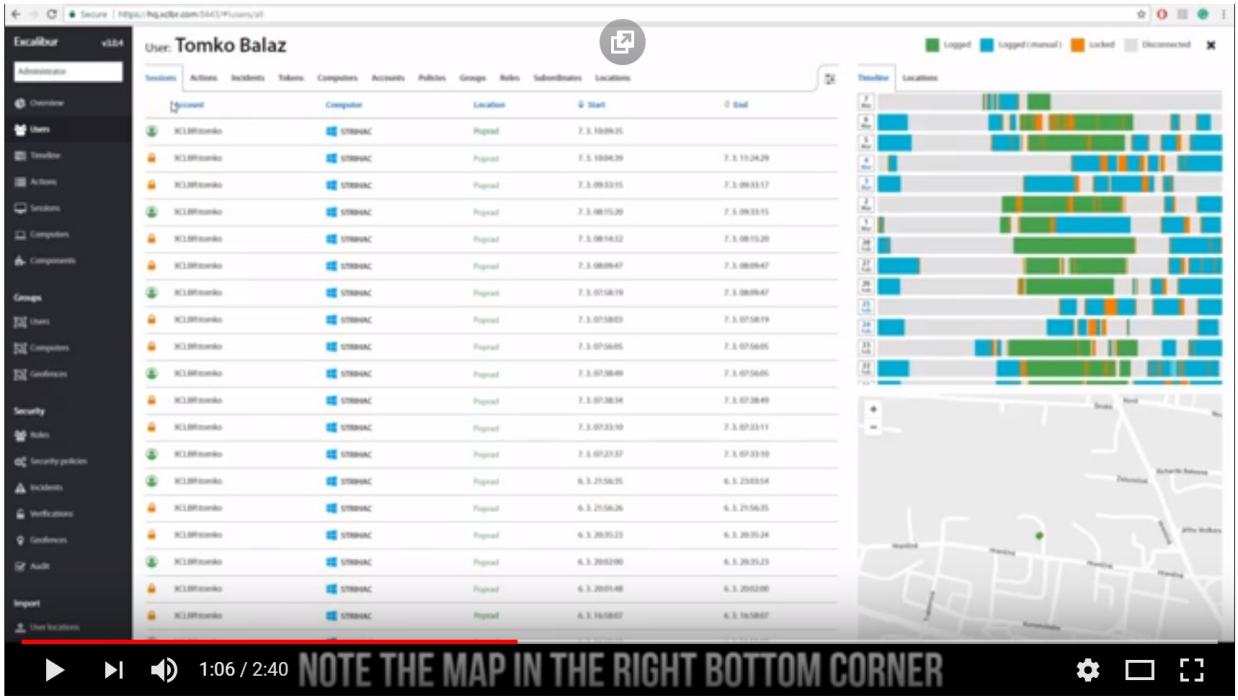
Face recognition can be trivially defeated using a picture or video, utilizing a real time video call the complexity of such an attack would be much greater. **A human can "recognize" even the best current deep-fakes** (aka deep neural network generated fake face videos), doing such a deep-fake video **real-time** based on a live conversation without a human detecting it seems to be **infeasible for at least the foreseeable future**. This way even a service-desk operator that doesn't know the person he is confirming can securely verify him – truly enabling a direct physical-trust based digital identity even with outsourced security operations centers **enabling novel security as a service business models**.

Contact: Ing. Ivan Klimek, PhD., CEO/CTO/Founder
mailto: ivan@xclbr.com
https://linkedin.com/in/ivanklimek

7. Timing

Everyone has a smartphone, but if they do not - Excalibur is backwards compatible and allows a gradual rollout – thus some users might still be left using older authentication mechanisms until they onboard.

Every action in Excalibur is cryptographically signed using the user phone's secure element and authentication factors used. Thus, it is impossible for the user to say – *"this wasn't me, Joe knew my password"*. Such level of auditability is unique to Excalibur and allows for a much stronger internal security posture and solves compliance problems. General Data Protection Regulation (GDPR) is just one of the reasons why enterprises and governments will invest more into internal security. Excalibur not only improves security and user experience but also **provides unparalleled visibility and control:** https://youtu.be/uRg8Ta2tQ8A



8. Stage

We have been working with the most technologically advanced bank (Tatra bank/Raiffeisen with 4000 internal users = employees) in Slovakia for the **past two years**. They are our first paying customer generating MRR. They are our showcase project – proving that **if Excalibur can make a whole bank password-free – it can make any enterprise password-free.** We also have a pilot running at **Volkswagen**. Now, it is just about replication / scaling.

9. Team / Company

We are a VC funded startup based in Slovakia. Our investors are Deutsche Telekom (T-Ventures / Hubraum), Neulogy Ventures and Credo Ventures. We have been working on Excalibur since 2013, first as a B2C product – to test our core technology on as many different setups as possible, and since 2015 as a B2B product. Our team consists of 10 senior software engineers and several more university interns.

Contact: Ing. Ivan Klimek, PhD., CEO/CTO/Founder
mailto: ivan@xclbr.com
https://linkedin.com/in/ivanklimek

10. Impact / Vision

Excalibur shows the way forward. The first step is to eliminate passwords in the enterprise because we have a pre-existing organizational structure that we can **bootstrap trust from**. But our goal is much bigger than that – **we want to make authentication completely transparent** - the correct user will not even know it is there – everything will just work, but for everyone else gaining access will be impossible. Exactly as in the legend about the sword Excalibur…

11. Further Materials

A brief two-pager is available here: https://getexcalibur.com/docs/excalibur_two_pager.pdf

A presentation showing Excalibur features / compatibility / UX / management is available for online viewing / download at: https://1drv.ms/p/s!AmqhF3qbTXHlgpUEnWjujAwQwVe-tw

Excalibur's whitepaper can be accessed here:
https://docs.google.com/document/d/1ED6J9_ZfHFogt0ROhAXssrbaUCoa-B5U5VjHCgnnCJM/edit?usp=sharing

12. Excalibur's History

Selected as a **finalist on the PwC Cybersecurity Day**, Luxembourg, October 2017

Winner of Volkswagen TechTalk 2017, Wolfsburg - **pilot project launch with VW**, August 2017

Excalibur launched pilot deployment at Tatrabanka, part of Raiffeisen Bank International – 2016 / 2017 – **our first paying customer, generating Monthly Returning Revenue (MRR)**

May 2016 - seed round - Neulogy Ventures - incorporated in Slovakia

Excalibur won the Kaspersky Security Startup Challenge at MIT In August 2015, after this we pivoted to full focus on B2B, this marks the start of Excalibur as an Enterprise solution

Excalibur got into the EIT ICT Berlin Residency 2014

Excalibur received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 684168

Excalibur won the Cisco IoT Security Grand Challenge 2014 - prize received directly from Cisco CTO

December 2013 - pre-seed - Deutsche Telekom (Hubraum) + Credo Ventures, incorporated in Poland

Excalibur got into the Intel Global Challenge 2013 at UC Berkeley

Excalibur got into the Telefonica Wayra startup accelerator 2013

Excalibur got into the finals of the Rice Business Plan Competition 2013

Excalibur won the Intel Business Challenge Europe 2013 (2nd place)

Excalibur won the Telekom Innovation Contest 2013 by Deutsche Telekom Group

World Intellectual Property Organization's Best Young Inventor 2013

Excalibur won the StartupAwards.SK DIGITAL 2012

Winner of the ITU Telecom World Young Innovators Competition 2012

Contact: Ing. Ivan Klimek, PhD., CEO/CTO/Founder
mailto: ivan@xclbr.com
https://linkedin.com/in/ivanklimek