ZealiD

Beyond Borders:

Revolutionizing Employee Experiences in the Digital Era

Contents

CHAPTER 1:

A New Beginning: The Evolution of Employee Onboarding

Summary

The evolution of employee onboarding in large enterprise companies over the past two decades showcases a significant shift from traditional paper-based methods to digital, automated, and remote-friendly processes. This transformation, driven by advancements in technology and changing workforce dynamics, has revolutionized how companies welcome and integrate new hires. Key milestones include the introduction of electronic forms and HR systems, the integration of applicant tracking systems, mobile-friendly onboarding experiences, the adoption of digital signatures for remote onboarding, and the incorporation of AI and automation tools. These developments have not only enhanced efficiency and organization but also provided greater flexibility and accessibility for both employees and employers. As companies continue to embrace digital innovation, the onboarding process will likely continue to evolve to meet the evolving needs of the modern workforce.

The onboarding process for employees in big enterprise companies has undergone significant evolution over the past 20 years, marked by several important milestones in transitioning from paper-based and physical methods to digital and remote processes. Here's an overview of key developments:

Paper-Based Processes (Early 2000s): Two decades ago, onboarding often involved manual, paper-based procedures. New hires would fill out paper forms for HR paperwork, tax forms, benefits enrollment, and other documentation. This process was time-consuming, prone to errors, and required physical storage space for records.

Introduction of Electronic Forms and HR Systems (Mid-2000s): As technology advanced, many companies began digitizing their onboarding processes by introducing electronic forms and HR management systems (HRMS). This allowed new hires to complete paperwork online, reducing paperwork and manual data entry for HR staff.

However, the process still often required in-person visits to submit physical documents and obtain signatures.

Integration of Applicant Tracking Systems (Late 2000s to Early 2010s): Applicant tracking systems (ATS) became more widely adopted, streamlining the recruitment and onboarding process. These systems allowed companies to manage job postings, applications, candidate communication, and onboarding tasks in a centralized digital platform, improving efficiency and organization.

Mobile-Friendly Onboarding (2010s): With the widespread adoption of smartphones and tablets, companies began offering mobile-friendly onboarding experiences. New hires could complete paperwork and training modules using their mobile devices, providing greater flexibility and accessibility.

Digital Signatures and Remote Onboarding (Mid-2010s): The introduction of digital signature technology facilitated the transition to remote onboarding. New hires could electronically sign documents from anywhere, eliminating the need for in-person visits and physical paperwork exchange. This allowed companies to onboard remote employees more efficiently and expanded their talent pool beyond geographic limitations.

AI and Automation (Late 2010s to Present): In recent years, artificial intelligence (AI) and automation have transformed the onboarding process further. AI-powered chatbots and virtual assistants can guide new hires through the onboarding process, answer questions, and provide personalized assistance. Automation tools streamline repetitive tasks, such as sending welcome emails, scheduling training sessions, and provisioning IT access, saving time for HR professionals and improving the new hire experience.

Overall, the onboarding process in big enterprise companies has evolved from manual, paper-based procedures to digital, automated, and remote-friendly workflows. This evolution has been driven by advancements in technology, changing workforce dynamics, and the need for greater efficiency and flexibility in talent management practices.

Example

Microsoft has long been a vanguard of innovation, a testament to its enduring commitment to progress spanning decades. This dedication has not only yielded groundbreaking external products but has also revolutionized internal company management practices, particularly in the realm of human resources workflows.

What was previously a cumbersome paper-based process has evolved over time into a streamlined digital experience. A significant milestone in this evolution was reached with the implementation of qualified electronic signatures, marking a pivotal breakthrough for the company. This innovative solution has facilitated Microsoft's transition to a singular, integrated platform, seamlessly encompassing operations across more than 12 European Union countries.

Actionable Insights

Embrace Digital Transformation: Companies should recognize the value of embracing digital transformation initiatives to modernize outdated processes. Transitioning from manual to digital workflows can enhance efficiency, accuracy, and overall productivity.

Invest in Innovation: Allocate resources towards innovation and technology adoption within organizational operations. Microsoft's success underscores the importance of investing in cutting-edge solutions to stay ahead of the curve and remain competitive in rapidly evolving markets.

Prioritize Employee Experience: Improving HR workflows not only benefits the organization but also enhances the overall employee experience. Companies should prioritize initiatives that streamline HR processes, making them more user-friendly, efficient, and conducive to employee satisfaction.

Pursue Global Integration: For multinational companies, pursuing global integration of HR systems can streamline operations and promote consistency across diverse geographic regions. Microsoft's implementation of a unified solution across multiple EU countries demonstrates the potential benefits of standardization on a global scale.

Compliance and Security: Ensure that any digital transformation initiatives comply with relevant regulations and prioritize data security. Qualified electronic signatures offer both efficiency and security benefits, but it's crucial to implement them in accordance with legal requirements and industry standards.

Continuous Improvement: Recognize that digital transformation is an ongoing journey rather than a one-time event. Continuously evaluate and refine HR workflows to leverage emerging technologies and best practices, ensuring that processes remain efficient, effective, and adaptable to evolving business needs.

Call to Action

Take a leap into digital transformation today. Embrace innovative solutions, prioritize employee experience, and commit to continuous improvement. Start now to streamline your HR processes and propel your organization towards sustainable growth.

CHAPTER 2:

Employee cloud interaction — The weak link in Cybersecurity

Summary

The main message highlights the various ways in which employees can inadvertently or intentionally become involved in cyberattacks, posing significant risks to organizations. Examples include falling victim to phishing scams, being manipulated through social engineering tactics, exploiting insider privileges for malicious purposes, having their credentials compromised, or engaging in deliberate malicious actions. Real-life instances, such as the DNC email compromise, the Twitter cryptocurrency scam, the Morgan Stanley data theft, the Equifax breach, and the Tesla employee hacking incident, underscore the severity of these threats and emphasize the importance of robust cybersecurity measures and employee awareness training to mitigate risks effectively.

Employees can unwittingly become involved in cyberattacks through various means, including phishing scams, social engineering tactics, insider threats, and compromised credentials. Here are some examples of how employees have been used in cyber- attacks in real life:

Phishing Attacks: Cybercriminals often use phishing emails to trick employees into revealing sensitive information or providing access to corporate networks. For example, an employee might receive an email purportedly from a trusted source, such as their company's IT department or a familiar vendor, requesting login credentials or asking them to click on a malicious link. In 2016, a phishing attack targeting employees at the Democratic National Committee (DNC) resulted in the compromise of thousands of emails and sensitive documents.

Social Engineering: Attackers may use social engineering techniques to manipulate employees into divulging confidential information or performing actions that compromise security. This could

involve impersonating a colleague or executive to gain trust or exploiting employees' natural inclination to help others. In 2019, a social engineering attack targeting Twitter employees resulted in the compromise of high-profile accounts, including those of Barack Obama and Elon Musk, as part of a cryptocurrency scam.

Insider Threats: Employees with privileged access to company systems or sensitive data can pose a significant threat if they misuse their access for malicious purposes. This could involve stealing data for financial gain, sabotage, or espionage. In 2014, an insider at Morgan Stanley stole confidential client data, including account numbers and contact information, with the intention of selling it to criminals.

Compromised Credentials: Cybercriminals may acquire employees' login credentials through various means, such as phishing, malware, or brute-force attacks. Once obtained, these credentials can be used to gain unauthorized access to corporate networks or sensitive systems. In 2017, the Equifax data breach, one of the largest breaches in history, was caused by hackers exploiting a vulnerability in the company's website to steal login credentials and access sensitive customer data.

Malicious Insider Actions: In some cases, employees may knowingly engage in malicious activities, either for personal gain or out of resentment towards their employer. This could involve intentionally leaking sensitive information, installing malware on company systems, or disrupting operations. In 2020, a former employee of Tesla was charged with hacking into the company's systems and transferring confidential data to third parties.

Example

The same company is using password-based credentials to allow employee access to internal systems.

Actionable Insights

Switching to certificate-based authentication decreases the possibility of successful cyber-attacks.

Call to Action

Build on the unified HR processes by extending the use of high assurance certificates for access provisioning.

CHAPTER 3:

Ensuring Workforce Legitimacy: Regulatory Imperatives and Employer Responsibilities

Summary

This chapter explores the rigorous regulatory requirements imposed by authorities worldwide on employers to verify the legitimacy of their workforce and uphold immigration laws. Beyond ensuring compliance, these regulations also aim to protect employees' rights, prevent exploitation, and maintain fair competition. Focusing on examples from the United States, United Kingdom, and various European Union (EU) member states such as Germany, France, Spain, and Italy, it elucidates the diverse approaches and obligations employers face in conducting background checks and verifying employee identification and work authorization. Failure to adhere to these regulations can result in severe penalties, emphasizing the critical need for employers to diligently uphold regulatory standards in the onboarding process.

Regulators worldwide impose stringent requirements on employers to ensure the legitimacy of their workforce and uphold immigration laws. Beyond these aims, these regulations also serve to protect employees' rights, prevent exploitation in the workforce, and maintain fair competition.

The Department of Homeland Security (DHS) in the United States mandates thorough background checks through the Form I-9 process to verify employees' identity and work authorization, with non-compliance resulting in severe penalties. Similarly, the United Kingdom enforces "right to work" rules, necessitating employers to verify employees' eligibility to work in the UK under threat of significant penalties. Within the European Union (EU), member states like Germany, France, Spain, and Italy impose similar obligations on employers to verify employees' identity and work authorization, aligning with their respective legislation and immigration laws. These requirements aim to

prevent unauthorized employment, safeguard national security, protect employees from exploitation, ensure workplace safety, and maintain fair competition. Failure to adhere to these regulations can lead to legal consequences and reputational damage for employers and lost opportunities for the employees, highlighting the imperative for strict adherence to regulatory standards in the onboarding process.

The Department of Homeland Security (DHS) in the United States has established stringent requirements for employers to conduct background checks as part of the employment eligibility verification process, commonly known as the Form I-9. This form requires employees to provide documentation to verify their identity and authorization to work in the United States. Employers are responsible for verifying the authenticity of the documents presented by employees and ensuring compliance with immigration laws. Failure to properly complete and retain Form I-9s can result in significant penalties for employers, including fines and legal consequences.

Similarly, in the United Kingdom, employers are subject to "right to work" rules, which require them to verify the identity and eligibility of employees to work in the UK. Employers must conduct thorough checks to ensure that employees have the legal right to work in the UK, which may include examining passports, visas, residence permits, or other documentation. The UK government provides guidance to employers on how to conduct these checks and maintain records to demonstrate compliance with immigration laws. Non-compliance with "right to work" rules can lead to severe penalties, including fines and criminal sanctions for employers.

In the European Union (EU), specific requirements for background checks and identification when onboarding new personnel can vary between member states. Here are examples from several EU countries:

Germany: In Germany, employers are required to verify the identity of new employees and ensure compliance with immigration laws. The Residence Act (Aufenthaltsgesetz) sets out rules for the employment of foreign nationals, including requirements for obtaining work permits and residence permits. Employers must conduct thorough checks to confirm the identity and eligibility of employees to work in Germany.

France: France has strict regulations governing the employment of foreign nationals. Employers are required to verify the identity and work authorization of new employees in compliance with the French Labor Code (Code du travail) and immigration laws. This may include conducting background checks and verifying the validity of work permits or residence permits.

United Kingdom: While the UK has left the EU, it still provides an example of background check and identification requirements. Employers in the UK are subject to "right to work" checks under the Immigration, Asylum and Nationality Act 2006. This legislation requires employers to verify the identity and work eligibility of employees by examining specified documents, such as passports, visas, or residence permits, before hiring them.

Spain: In Spain, employers must comply with regulations regarding the employment of foreign nationals, as outlined in the Foreigners Act (Ley de Extranjería). Employers are responsible for verifying the identity and work authorization of new employees and ensuring compliance with immigration laws. This may involve conducting background checks and obtaining work permits or residence permits for foreign employees.

Italy: Italy has regulations governing the employment of foreign nationals under the Consolidated Immigration Act (Testo Unico sull'Immigrazione). Employers are required to verify the identity and work authorization of new employees and ensure compliance with immigration laws. Background checks may be conducted as part of the hiring process to confirm the eligibility of employees to work in Italy.

These examples demonstrate how EU countries implement background check and identification requirements for onboarding new personnel in accordance with their respective legislation, regulations, and authority requirements. Employers operating in EU member states should familiarize themselves with the specific legal and regulatory obligations applicable in each country where they operate.

Example

Microsoft utilizes a qualified electronic signature solution to navigate EU regulatory variations. Beginning with the signing of employment agreements, the process extends to fulfilling diverse background checks like the right to work. Identity wallets serve as a centralized platform for employers and employees to manage their professional relationship efficiently.

Actionable Insights

Streamline Compliance Processes: Implementing a qualified electronic signature solution can streamline compliance efforts, especially in regions with diverse regulatory frameworks like the EU. This not only ensures legal adherence but also reduces administrative burden.

Enhance Onboarding Efficiency: By starting the employment journey with electronic signatures, organizations can expedite the onboarding process. This efficiency improvement can positively impact productivity and employee satisfaction.

Centralize Management with Identity Wallets: Leveraging identity wallets offers a centralized platform for managing various aspects of the employer-employee relationship. This includes facilitating background checks and other necessary documentation, leading to smoother operations.

Ensure Data Security: Prioritize data security measures within electronic signature and identity wallet systems to safeguard sensitive information. This can mitigate risks associated with identity theft or unauthorized access.

Adaptability to Global Operations: Companies operating across multiple jurisdictions can benefit from solutions that accommodate diverse regulatory requirements. Ensuring scalability and adaptability to different legal environments is crucial for sustainable growth.

Call to Action

Implement an integrated electronic signature and identity wallet solution to streamline compliance processes and enhance efficiency in managing employee relationships across diverse regulatory landscapes like the EU.

CHAPTER 4:

EU Regulated Identity and standards to the rescue

Summary

The chapter provides an overview of the eIDAS regulation established by the EU, outlining the framework for electronic identities (eIDs) and qualified certificates. eIDs, issued by government entities or certified private organizations, enable individuals to authenticate themselves electronically across borders within the EU, ensuring interoperability and security. Qualified certificates, issued by qualified trust service providers, authenticate individuals, organizations, or electronic systems in electronic transactions, adhering to stringent technical and security standards set by ETSI and eIDAS. The chapter delineates the creation processes for qualified certificates, highlighting two methods: eID high assurance and certified registration processes. Despite challenges in accessing eIDs, advancements in technology have facilitated the issuance of regulated eIDAS identities globally. Overall, eIDAS and ETSI standards establish a robust framework for electronic identities and qualified certificates, fostering trust, security, and interoperability in electronic transactions across the EU.

The eIDAS (Electronic Identification, Authentication, and Trust Services) regulation, established by the European Union (EU), has indeed created a framework for two types of regulated identities: electronic identities (eIDs) and qualified certificates. These identities are underpinned by global standards set by the European Telecommunications Standards Institute (ETSI).

Electronic Identities (eIDs): eIDs are digital identities issued by EU member states' governments or certified private entities. They serve as a means for individuals to authenticate themselves electronically in various online transactions and interactions with public services and private organizations. eIDs provide a standardized and secure way for individuals to prove their identity online across borders within the EU. The use of eIDs is regulated by eIDAS to ensure interoperability, security, and trustworthiness.

Qualified Certificates: Qualified certificates are digital certificates issued by qualified trust service providers (QTSPs) in accordance with eIDAS regulations. These certificates are used to authenticate the identity of individuals,

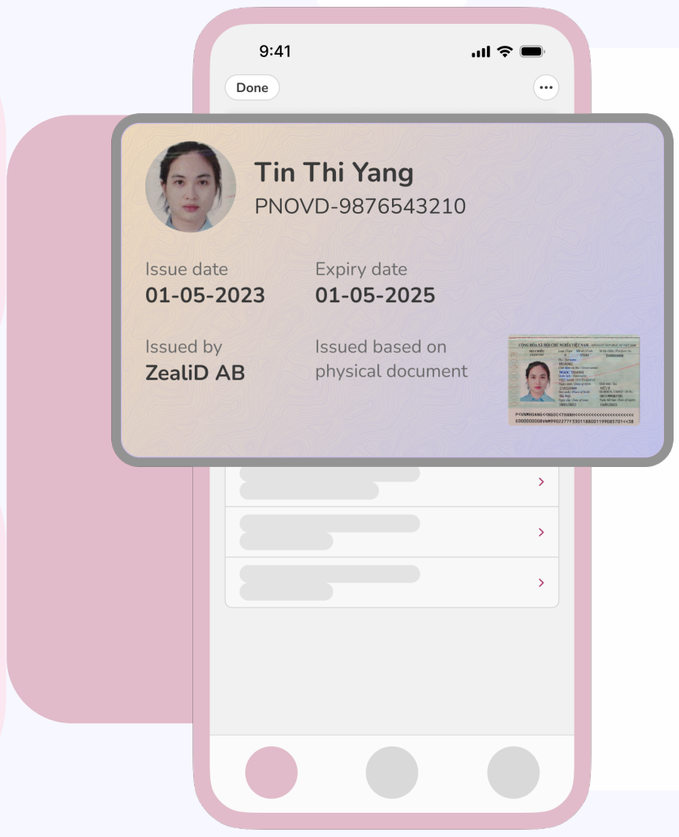
authenticate the identity of individuals, organizations, or electronic systems in electronic transactions and communications. Qualified certificates adhere to strict technical and security requirements defined by eIDAS and ETSI standards to ensure their reliability and legal validity across the EU. They are typically issued following a certified registration process conducted by qualified trust service providers.

The creation and issuance of qualified certificates are governed by ETSI standards, particularly ETSI EN 319 409 and ETSI EN 319 411, which define the technical specifications and security requirements for qualified electronic signatures, seals, timestamps, and certificates. Additionally, ETSI TS 119 461 specifies the requirements for the creation of qualified certificates based on eID high assurance or a certified registration process.

Under ETSI TS 119 461, qualified certificates can be created based on either:

1. **eID High Assurance:** In this approach, eIDs issued by EU member states' governments are utilized as a high-assurance means of identity verification. The eIDAS regulation ensures that these eIDs meet specific security and assurance levels, making them suitable for creating qualified certificates. In general this is still problematic as most of EUs citizen's lack digital access to an eID. eIDs with high level of assurance cannot be issued remotely as a rule, and can only be issued to citizen's of a member state.
2. **Certified Registration Process:** Alternatively, qualified certificates can be issued based on a certified registration process conducted by qualified trust service providers. This process involves verifying the identity of the certificate holder through reliable and secure means, following the requirements specified in ETSI 119 461. With the advent of smartphones and machine computing, these methods have evolved quickly. Today any citizen globally can in minutes get a regulated eIDAS identity from e.g. ZealiD.

Overall, eIDAS and ETSI standards establish a robust framework for electronic identities and qualified certificates, ensuring trust, security, and interoperability in electronic transactions across the EU.



CHAPTER 5:

New kid on the block: Decentralized Identity

Summary

Decentralized identity empowers individuals to control their identity data without central authorities. Major players like Microsoft Entra advocate for interoperability and standards to ensure widespread adoption. Through technologies like verifiable credentials and decentralized identifiers (DIDs), they aim to integrate seamlessly with existing systems while prioritizing privacy and security. This chapter explores the transformative impact of decentralized identity, putting individuals in control and reducing the risk of data breaches.

Decentralized identity refers to a digital identity model where individuals have control over their own identity information without relying on central authorities or intermediaries. In this model, individuals store their identity data securely on their own devices or in decentralized networks, such as blockchain, and can selectively share this information with others as needed. Decentralized identity empowers individuals to manage and authenticate their identities across various online services and platforms while ensuring privacy, security, and user-centric control.

Although there has been much discussion about this in the past years we are now seeing big tech are moving in and positioning themselves in decentralized identity. Microsoft Entra recognizes the potential of decentralized identity as a transformative approach to digital identity management. They emphasize the importance of interoperability and standards in ensuring widespread adoption of decentralized identity solutions. By leveraging technologies such as verifiable credentials and decentralized identifiers

(DIDs), Microsoft Entra aims to enable seamless integration with existing identity systems and platforms, thereby facilitating secure and privacy-preserving identity interactions across the digital landscape. They advocate for collaborative efforts within the industry to develop open standards and protocols that support decentralized identity ecosystems, fostering innovation and empowering individuals to fully control their digital identities.

Most importantly, this paradigm shift places the individual, holder of the credentials and the centre of the whole infrastructure. The change significantly decreases the risk of honeypot data troves held by companies being attacked and leaked. Whereas the individual receives granular control over the identity attributes that have been shared.

CHAPTER 6:

Unlocking Mobility: From regulated identity to Seamless Collaboration Across Clouds with hybrid identity wallets

Summary

The future of digital identity management lies in combining government-regulated systems with decentralized solutions, as advocated by Microsoft Entra. This hybrid approach balances regulatory compliance with decentralized control, ensuring enhanced privacy, security, and user autonomy. It enables individuals to securely manage their identity data while complying with regulations and simplifying processes such as employee onboarding, access management, remote work verification, compliance assurance, and credential management. Collaboration is key to developing open standards supporting interoperability, fostering innovation, and creating a more secure and user-centric digital identity landscape.

The convergence of government-regulated identity systems and decentralized identity solutions, as advocated by Microsoft Entra, represents the future of digital identity management. This hybrid approach acknowledges the need for regulatory oversight and protection while harnessing the benefits of decentralization for enhanced privacy, security, and user control.

Government-regulated identity systems provide a framework for ensuring compliance with legal requirements, protecting against identity theft, and safeguarding sensitive personal information. However, these centralized systems often face challenges such as single points of failure, data breaches, and lack of user control over their own identity data.

On the other hand, decentralized identity solutions offer a promising alternative by shifting the control

of identity data back to individuals. With technologies like verifiable credentials and decentralized identifiers, individuals can securely store and manage their identity information, selectively sharing it with trusted parties as needed. This approach minimizes the risk of data breaches and unauthorized access, while also empowering users to maintain greater autonomy over their digital identities.

By integrating government-regulated identity systems with decentralized identity solutions, a hybrid model emerges that combines the strengths of both approaches. Individuals can maintain a digital wallet containing both government-issued credentials and decentralized identifiers, allowing them to seamlessly navigate between regulated and decentralized identity ecosystems. This interoperability ensures compliance with regulatory requirements while enabling innovative use cases and empowering individuals to fully control their digital identities.

In this hybrid future, collaborative efforts between governments, tech companies, and industry stakeholders will be essential to develop open standards and protocols that support interoperability and compatibility between different identity systems. By embracing this hybrid approach, we can create a more secure, privacy-preserving, and user-centric digital identity landscape that benefits both individuals and society as a whole.

Here are some important use cases that are solved by Identity wallets founded in regulated identity but with flexibility of verified credentials:

Here are some important use cases that are solved by Identity wallets founded in regulated identity but with flexibility of verified credentials:

1. **Employee Onboarding:** A hybrid wallet can streamline the onboarding process by allowing employees to securely store and share their identity documents and credentials with HR departments or hiring managers. This eliminates the need for physical document submission and manual verification, reducing administrative burden and improving the overall onboarding experience.

2. **Access Management:** Hybrid wallets can enhance access management processes within organizations by providing employees with a secure and convenient way to authenticate their identities for accessing company systems, applications, and physical spaces. This ensures that only authorized personnel can access sensitive data or restricted areas, thereby bolstering security measures while simplifying user authentication.

3. **Remote Work Verification:** With the rise of remote work, verifying employees' identities and ensuring compliance with company policies becomes increasingly crucial. A hybrid wallet can enable employees to securely authenticate their identities when logging into remote work systems or participating in virtual meetings, ensuring that only authorized personnel can access company resources from remote locations.

4. **Compliance Verification:** In industries where regulatory compliance is paramount, such as finance or healthcare, hybrid wallets can facilitate compliance verification processes by securely storing and sharing employees' credentials and certifications. This ensures that organizations maintain compliance with industry regulations while streamlining the verification process for employees and regulatory authorities alike.

5. **Credential Management:** Managing various professional credentials, licenses, and certifications can be cumbersome for employees. A hybrid wallet can serve as a centralized repository for storing and managing these credentials, allowing employees to easily access and share them when needed for professional purposes, such as applying for new positions or attending industry conferences. This improves efficiency and reduces the risk of credential loss or mismanagement.

ZealiD

2024

Content by ZealiD

Illustrations by Storyset