Digitizing Academic Credentials with Microsoft Entra Verified ID

Integrating Digital Education strategy with Identity programs like the UK Digital Wallet

Executive Summary

Education organizations can leverage Microsoft Entra Verified ID, a decentralized identity management solution, to create a platform for issuing, managing, and verifying digital academic credentials that can be stored in the GOV.UK Wallet.

This approach aligns with the UK's push toward secure, user-controlled digital identities and integrates with the GOV.UK One Login system, as outlined in recent government initiatives.

Education Verified ID

Education organizations can leverage Microsoft Entra Verified ID, a decentralized identity management solution, to create a platform for issuing, managing, and verifying digital academic credentials that can be stored in the GOV.UK Wallet.

This approach aligns with the UK's push toward secure, user-controlled digital identities and integrates with the GOV.UK One Login system, as outlined in recent government initiatives.

1. Understanding Microsoft Entra Verified ID and GOV.UK Wallet

- **Microsoft Entra Verified ID**: This is a verifiable credential service built on open standards, enabling organizations to issue digital credentials that users store in digital wallets. These credentials are cryptographically signed, ensuring security, privacy, and verifiability. It supports user-owned identity scenarios, allowing individuals to control what data they share and with whom.
- **GOV.UK Wallet**: Scheduled for launch in summer 2025, the GOV.UK Wallet is a digital identity wallet that allows UK residents to store government-issued documents, such as digital driving licenses and Veteran Cards, on their smartphones. It is underpinned by GOV.UK One Login, which provides secure identity verification. The wallet aims to support additional credentials, including those from certified third parties, by 2027.

2. Steps for Education Organizations to Build a Platform with Microsoft Entra Verified ID

Education organizations can follow these steps to create a platform for digitizing academic credentials compatible with the GOV.UK Wallet:

Step 1: Define Credential Types and Standards

- **Identify Credential Types**: Determine the academic credentials to digitize, such as diplomas, transcripts, certificates, or micro-credentials (e.g., course completions, skills badges). These should align with standards like the 1EdTech Comprehensive Learner Record (CLR) or Open Badges for interoperability.

- **Adopt Open Standards**: Use standards like W3C Verifiable Credentials and Open Badges 3.0 to ensure credentials are machine-readable, secure, and interoperable with digital wallets, including the GOV.UK Wallet. Microsoft Entra Verified ID is built on these standards, making it suitable for this purpose.

Step 2: Configure Microsoft Entra Verified ID

- **Set Up Entra Verified ID**: Education organizations can configure Entra Verified ID through the Microsoft Entra admin center. This involves creating templates for credentials (e.g., degree certificates) with metadata like program name, issuance date, and skills demonstrated. Templates can be branded with the institution's logo for recognition.
- **Integration with Existing Systems**: Use Microsoft's APIs and SDKs to integrate Entra Verified ID with student information systems (SIS) or learning management systems (LMS). This allows seamless issuance of credentials upon course completion or degree conferral. For example, the UK Department for Education (DfE) prototyped a solution with Entra Verified ID to streamline student credential verification.
- **Privacy and Control**: Ensure credentials respect user privacy by requiring user approval for sharing. Entra Verified ID allows users to store credentials in a digital wallet (e.g., Microsoft Authenticator or another compatible wallet) and selectively share data, aligning with GOV.UK Wallet's user-controlled model.

Step 3: Issue Verifiable Credentials

- **Credential Issuance Process**: When a student completes a program, the institution issues a verifiable credential via Entra Verified ID. The credential is cryptographically signed and sent to the student's digital wallet. For example, a university could issue a digital diploma containing the degree title, conferral date, and recipient's identity, verifiable by third parties.
- **User Storage**: Students store these credentials in a digital wallet, such as Microsoft Authenticator or, potentially, the GOV.UK Wallet if certified for third-party credentials. The GOV.UK Wallet's integration with GOV.UK One Login ensures secure access,

and organizations certified under the UK Digital Identity and Attributes Trust Framework can issue compatible credentials.

Step 4: Enable Verification for Stakeholders

- **Verification Process**: Employers, other educational institutions, or government agencies can verify credentials using Entra Verified ID's verification tools. For instance, a university can confirm a student's transcript in minutes by scanning a QR code or accessing a shared credential, reducing verification time from weeks to hours, as demonstrated by the DfE.
- **Integration with GOV.UK Wallet**: Organizations certified under the UK's Digital Identity and Attributes Trust Framework can access credentials stored in the GOV.UK Wallet, provided the user consents. This enables seamless verification for purposes like employment, further education, or government services (e.g., proving qualifications for benefits).

Step 5: Ensure Interoperability with GOV.UK Wallet

- **Trust Framework Compliance**: To integrate with the GOV.UK Wallet, education organizations must be certified under the UK Digital Identity and Attributes Trust Framework. This involves adhering to standards for security, privacy, and interoperability, as outlined in the Data (Use and Access) Bill.
- **Derived Credentials**: Organizations can create "derived credentials" (e.g., a simplified credential proving a specific qualification) that can be stored in the GOV.UK Wallet for specific use cases, such as proving eligibility for a job or age-restricted services.
- **Collaboration with GOV.UK**: Engage with the Government Digital Service (GDS) to ensure credentials are compatible with the GOV.UK Wallet. The GDS is open to collaboration with third parties to expand the wallet's capabilities, as noted in their engagement with the technology sector.

Step 6: Enhance Security and Accessibility

- **Security Features**: Use Entra Verified ID's Face Check and biometric integration (aligned with GOV.UK Wallet's facial recognition capabilities) to ensure credentials are securely tied to the rightful owner. This prevents fraud and aligns with the wallet's security measures.

- **Accessibility**: Provide web-based access to credentials for users without smartphones, as MIT's Digital Credentials Consortium suggests, to ensure inclusivity. Entra Verified ID supports flexible deployment options to accommodate diverse users.

3. Benefits for Education Organizations

- **Efficiency**: Automating credential issuance and verification reduces administrative burdens. The DfE reported cutting verification times from weeks to hours using Entra Verified ID.
- **Cost Savings**: Standardizing credential systems could save significant costs, with the DfE estimating £300 million in savings across UK universities.
- **Student Empowerment**: Students control their credentials, sharing only necessary data with employers or institutions, enhancing privacy and user agency.
- **Fraud Prevention**: Cryptographic signatures and real-time verification reduce credential fraud, a key benefit highlighted by European Digital Credentials and the GOV.UK Wallet.
- **Interoperability**: Credentials issued via Entra Verified ID can potentially be used across global platforms, aligning with EU standards and supporting international mobility.

4. Challenges and Considerations

- **Certification Requirements**: Organizations must be certified under the UK Trust Framework to integrate with the GOV.UK Wallet, which may involve compliance costs and audits.
- **Adoption Barriers**: Students and institutions may need training to adopt digital wallets. The DfE emphasized user consultation to ensure usability.
- **Privacy Concerns**: While Entra Verified ID and GOV.UK Wallet prioritize user control, data breaches could expose sensitive information, as noted by security experts. Robust encryption and compliance with GDPR are critical.

- **Interoperability with GOV.UK Wallet**: The GOV.UK Wallet currently prioritizes government-issued documents, and third-party credential support is still evolving. Early engagement with GDS is essential to ensure compatibility.

5. Practical Example: UK Department for Education Case Study

The UK Department for Education (DfE) partnered with Microsoft and Methods to prototype a digital credential system using Entra Verified ID. The system allowed students to apply to programs in minutes, with verification times reduced from weeks to hours. Students stored credentials in a branded digital wallet, and the solution integrated with existing systems, demonstrating scalability and user trust. This model can be adapted by other education organizations to issue credentials compatible with the GOV.UK Wallet, provided they meet Trust Framework standards.

6. Next Steps for Education Organizations

- **Pilot a Solution**: Start with a small-scale pilot, as the DfE did, to test credential issuance and verification using Entra Verified ID.
- **Engage with GDS**: Contact gov.uk.wallet-queries@digital.cabinet-office.gov.uk to participate in user research and ensure alignment with GOV.UK Wallet specifications.
- **Leverage Microsoft Resources**: Use Microsoft’s developer kits, APIs, and documentation to build and customize the platform. The Entra Wallet Library demo app provides a starting point for mobile integration.
- **Ensure Compliance**: Work toward certification under the UK Digital Identity and Attributes Trust Framework to enable integration with the GOV.UK Wallet.

Conclusion

By using Microsoft Entra Verified ID, education organizations can create a secure, user-controlled platform for issuing digital academic credentials that align with the GOV.UK Wallet’s framework. This involves configuring Entra Verified ID, issuing verifiable credentials, ensuring Trust Framework compliance, and integrating with existing systems.

The result is a streamlined, fraud-resistant system that empowers students, reduces administrative costs, and supports the UK’s digital identity vision. For further details on Entra Verified ID, visit Microsoft’s official documentation. For GOV.UK Wallet collaboration, reach out to the Government Digital Service.

Digital Education

The UK Department for Education (DfE) partnered with Microsoft and Methods, a digital transformation consultancy, to prototype a digital credential system using **Microsoft Entra Verified ID**.

This initiative aimed to modernize the issuance, storage, and verification of academic credentials, addressing inefficiencies in traditional paper-based processes. Below is an expanded explanation of this prototype, including its objectives, implementation, outcomes, and relevance to education organizations seeking to digitize credentials for compatibility with platforms like the GOV.UK Wallet.

Background and Objectives

The DfE's prototype was part of broader efforts to streamline education processes and align with the UK's digital identity strategy, particularly the **UK Digital Identity and Attributes Trust Framework** and the forthcoming **GOV.UK Wallet** (set to launch in summer 2025). The key objectives were:

- **Reduce Administrative Burden**: Traditional credential verification (e.g., degree certificates) often takes weeks, involving manual checks and third-party agencies. The DfE sought to cut this to hours or minutes.
- **Enhance Accessibility**: Enable students to store and share credentials securely in a digital wallet, giving them control over their data.
- **Prevent Fraud**: Address credential fraud (e.g., fake diplomas) by using cryptographically secure verifiable credentials.
- **Support Scalability**: Create a model that universities and other education providers could adopt nationwide, potentially saving £300 million annually across UK higher education, as estimated by the DfE.
- **Align with Digital Identity Goals**: Ensure compatibility with emerging digital identity systems, such as the GOV.UK Wallet, to support seamless integration with government and private-sector services.

Implementation Details

The prototype leveraged **Microsoft Entra Verified ID**, a decentralized identity platform built on **W3C Verifiable Credentials** standards, to issue, store, and verify academic credentials. Here's how it was implemented:

- **Credential Issuance**:
    - **System Integration**: The DfE worked with Methods to integrate Entra Verified ID with a simulated student information system (SIS), mimicking platforms like SITS or Banner used by universities. This allowed automatic issuance of credentials upon course completion or degree conferral.
    - **Credential Types**: The prototype focused on issuing digital versions of degree certificates, transcripts, and micro-credentials (e.g., course completion badges). Each credential included metadata such as the student's name, degree title, issuance date, and institution.
    - **Branding and Trust**: Credentials were digitally signed using Entra Verified ID's cryptographic capabilities, ensuring authenticity. They were branded with the issuing institution's logo, enhancing recognizability.
- **Storage in Digital Wallets**:
    - **User Control**: Students received credentials in a digital wallet, such as **Microsoft Authenticator**, which supports Entra Verified ID. This allowed students to store credentials securely on their smartphones and control what data to share.
    - **Privacy Features**: Entra Verified ID enabled selective disclosure, meaning students could share specific attributes (e.g., proof of degree completion) without revealing sensitive details (e.g., grades or personal identifiers).
- **Verification Process**:
    - **Real-Time Verification**: Employers, universities, or other relying parties could verify credentials instantly by scanning a QR code or accessing a shared credential link. Entra Verified ID's decentralized identifier (DID) framework ensured verifiers could trust the credential without contacting the issuing institution directly.
    - **Streamlined Workflow**: The prototype reduced verification times from weeks (common with paper-based processes) to hours or minutes, as verifiers could

check credentials against a decentralized ledger or Entra's verification service.

- **Technical Setup**:
    - **Microsoft Azure Integration**: The system used Azure Active Directory (now part of Microsoft Entra) for identity management, ensuring secure authentication of students and institutions.
    - **APIs and SDKs**: Methods utilized Microsoft's APIs and SDKs to customize the platform, integrating it with existing education systems and ensuring scalability.
    - **Standards Compliance**: The prototype adhered to **W3C Verifiable Credentials** and **OpenID for Verifiable Credentials**, aligning with global standards and enabling potential interoperability with systems like the EU's **EUDI Wallet**.
- **User Experience**:
    - **Branded Wallet**: The DfE created a branded digital wallet interface for students, improving user trust and engagement. This was critical, as user adoption is a key challenge for digital identity systems.
    - **Accessibility**: The prototype included web-based access options to ensure inclusivity for users without smartphones, addressing concerns raised by initiatives like MIT's Digital Credentials Consortium.

Outcomes and Impact

The DfE's prototype demonstrated significant potential for transforming academic credential management:

- **Efficiency Gains**: Verification times dropped from weeks to hours or minutes, as reported by the DfE. For example, a student applying for a job could share a digital degree certificate, which an employer verified instantly via Entra Verified ID.
- **Cost Savings**: By reducing manual processes and third-party verification services, the DfE estimated potential savings of £300 million annually if scaled across UK higher education institutions.

- **Fraud Reduction**: Cryptographic signatures made credentials tamper-proof, addressing issues like diploma fraud, which affects millions globally, according to European Commission reports.
- **Student Empowerment**: Students gained control over their credentials, sharing only necessary data with employers or institutions, aligning with GDPR and privacy-by-design principles.
- **Scalability**: The prototype proved adaptable for various credential types (e.g., degrees, micro-credentials) and integrable with existing systems, making it a viable model for widespread adoption.

Relevance to GOV.UK Wallet

The DfE's prototype is highly relevant to education organizations aiming to issue credentials compatible with the **GOV.UK Wallet**:

- **Standards Alignment**: The use of W3C Verifiable Credentials ensures compatibility with the GOV.UK Wallet, which is built to support third-party credentials under the UK Digital Identity and Attributes Trust Framework.
- **Certification Pathway**: Institutions adopting a similar model must become certified under the UK Trust Framework to issue credentials for the GOV.UK Wallet. The DfE's prototype provides a blueprint for meeting these requirements.
- **User-Centric Design**: The branded wallet and selective disclosure features align with the GOV.UK Wallet's focus on user control and privacy, as emphasized by the Government Digital Service (GDS).
- **Potential Interoperability**: While the GOV.UK Wallet initially prioritizes government-issued documents (e.g., driving licenses), its planned expansion to third-party credentials by 2027 makes the DfE's model a forward-compatible solution.

Lessons for Education Organizations

Education organizations can draw several lessons from the DfE's prototype when building their own platforms:

- **Leverage Existing Systems**: Integrate Entra Verified ID with SIS or LMS platforms to automate credential issuance, as demonstrated by the DfE’s integration with a simulated SIS.
- **Prioritize User Experience**: Create branded, user-friendly wallets and provide web-based access to ensure inclusivity, as seen in the prototype’s design.
- **Engage Stakeholders**: Collaborate with employers and other institutions to ensure verification processes meet their needs, as the DfE did to streamline job applications.
- **Plan for Scalability**: Design systems that can handle diverse credential types and scale across institutions, as shown by the prototype’s adaptability.
- **Align with Standards**: Use W3C Verifiable Credentials and comply with the UK Trust Framework to ensure compatibility with the GOV.UK Wallet and potential EU interoperability.

Challenges and Considerations

- **Adoption Barriers**: The DfE noted that user training is essential, as students and staff may be unfamiliar with digital wallets. User consultation, as conducted in the prototype, is critical.
- **Certification Costs**: Becoming a certified issuer under the UK Trust Framework involves compliance costs, which smaller institutions may find challenging.
- **Interoperability with GOV.UK Wallet**: While the prototype’s credentials are technically compatible, the GOV.UK Wallet’s third-party support is still developing. Early engagement with GDS (via gov.uk.wallet-queries@digital.cabinet-office.gov.uk) is necessary.
- **Security**: Despite robust encryption, data breaches remain a risk, as highlighted by security experts. Institutions must implement strong safeguards, as the DfE did with Azure’s security features.

Broader Implications

The DfE’s prototype serves as a proof of concept for education organizations worldwide. Its success has inspired similar initiatives, such as the **European Blockchain Services**

Infrastructure (EBSI), which pilots digital diplomas using similar technologies. For UK institutions, the prototype highlights a path to integrate with the GOV.UK Wallet while maintaining compatibility with global standards like those of the EU’s EUDI Wallet. By adopting Entra Verified ID, institutions can issue credentials that are secure, user-controlled, and verifiable, supporting both domestic and international use cases.

Next Steps for Education Organizations

- **Pilot a Similar System**: Start with a small-scale pilot, as the DfE did, to test Entra Verified ID with a specific credential type (e.g., micro-credentials).
- **Collaborate with Microsoft and Partners**: Work with Microsoft or consultancies like Methods to customize Entra Verified ID for institutional needs.
- **Engage with GDS**: Contact the Government Digital Service to align with GOV.UK Wallet specifications and participate in user research.
- **Monitor EU Developments**: Given potential UK-EU digital identity alignment, ensure credentials are eIDAS-compliant for cross-border use.

For further details, refer to Microsoft’s **Entra Verified ID documentation** or contact the GDS for GOV.UK Wallet integration guidance. The DfE’s prototype underscores the transformative potential of digital credentials, offering a practical model for education organizations to follow.