Digital Credentials in SA



PrivySeal® was founded to make genuine qualifications & licensing visible.

The problem of fraudulent qualifications remains significant.

National Qualifications Framework Amendment Act creates two registers.

Credentials take different forms - currently most are PDF / printed (think of the current driver's license, regulatory licensing and graduation certificates).

PrivySeal® has been helping Issuers like SAQA, ZAQA, SACAP, SACQSP, SACSSP and many others to migrate to digital credentials since 2016.

The migration process from paper / PDF to digital requires the buy-in of the Issuers.

Do not forget that the Issuers will continue to be key in any credential issuing process.





Making credentials visible is important for many reasons.

Scan the QR code on the example PrivySeal® (micro-credential) to access the encrypted digital certificate (credential).





PrivySeal® are added to email. footers, websites, documents. Financial statements, Plans...



09:09 AM (Africa/Johannesburg) on 01 Mar 2022

PROFESSIONAL QUANTITY SURVEYOR



09:03 AM (Africa/Johannesburg) on 01 Mar 2022





PROFESSIONAL ARCHITECT



09:00 AM (Africa/Johannesburg) on 01 Mar 2022

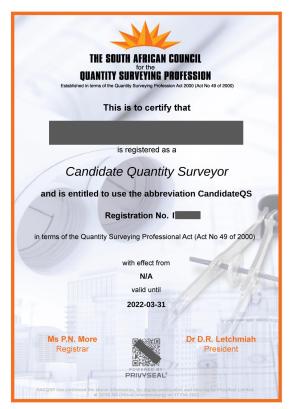
QR codes links to real-time digital credential.

SACAP requires Architectural Professionals to add their PrivySeal® to their Plans to reduce fraud.

Real-time credentialing - confirming genuine qualifications & licensing







Issuer buy-in



Issuers must be able to trust that their data is not going to be compromised and that they will be able to securely update or even revoke the digital credential.

Currently PrivySeal[®] clients control their data centrally and the credentials change in real-time as they update their records. This gives Issuers comfort as their control over the credential is increased.

Further tightening controls by using cryptographic keys, allows the Issuer to trust a new de-centralised architecture, where the cryptography potentially "underwrites" the risk of fraud.

Data Interoperability builds confidence (PrivySeal® suggests open standards such as JSON).

Data Privacy can further reassure the Issuer that the new credentials will not be abused.

Issuers of such a cryptographic credentials may agree to using a decentralised infrastructure where they do not have the same degree of control.

Data interoperability learnings



- Beware bespoke (platform specific) data schemas.
- Consider using the tried and tested JSON open standard (ISO/IEC 21778:2017).
- \triangleright Use APIs to collect data & avoid having to parse data (f/n=firstname..).
- Beware IT protocols that are contested.

Data privacy questions



- Does PSET CLOUD have the data subjects express permission to process & generate data?
- Does PSET CLOUD use data in the normal course, as the data subject would expect?
- Does PSET CLOUD combine different datasets when processing data?
- How intrusive, predictive or potentially damaging is the data modelling?
- > Consider engineering safeguards to avoid unintended consequences.