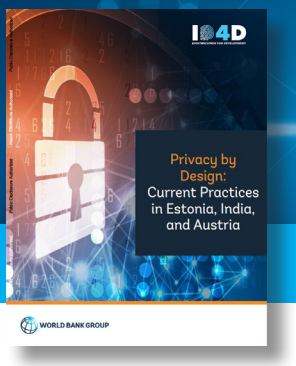
WORLD BANK GROUP

ID4D
IDENTIFICATION FOR DEVELOPMENT

PRIVACY BY DESIGN: CURRENT PRACTICES IN ESTONIA, INDIA, AND AUSTRIA

RESEARCH SUMMARY

id4d.worldbank.org



BACKGROUND

Digital ID systems can play a transformational role across many sectors yet—as with any system that collects, uses, and stores personal data—they also create challenges for privacy and data protection.[1] As highlighted in the *Principles on Identification*[2], protecting personal data in ID systems requires not only a comprehensive legal framework, but also a **"privacy—and-security-by-design" (PbD) approach**[3] that:

1. **Develops proactive—not reactive—systems** that take a preventative not remedial approach;
2. **Makes privacy the default setting**, rather than requiring affirmative action;
3. **Embeds privacy into the technical design** from the start rather than retrofitting it;
4. **Views privacy in a positive-sum manner** ("win-win"), and not as a zero-sum ("either/or");
5. **Develops end-to-end security** with a view to full-lifecycle protection;
6. **Builds-in visibility and transparency** and keeping systems open and accountable; and
7. **Keeps the system user-centric,** with an eye to respecting user data privacy.

In order to understand current PbD practices in digital ID systems, a recent ID4D paper explores different legal, operational, and technical controls used by in Estonia, India, and Austria.[4]

ESTONIA – PbD example: Estonia's Citizen Portal

Estonia's citizen portal (eesti.ee) provides users with multiple tools to oversee and control their data. First, it allows users to see who has accessed their data via the Personal Data Usage Monitor[5] that logs all transactions containing personal data. A user can check these logs for any unauthorized usage of their data, and then contest any unsanctioned access. Second, it gives users the ability to control which data is shared with whom. With health services, for example, patients can view all their electronic health records (EHRs) through the Estonian eHealth Patient Portal, and selectively share them with providers after authenticating their identity with their digital ID.

INDIA – PbD example: India's Virtual ID and Tokenization

The Aadhaar ID system offers multiple features that enhance privacy including (a) Virtual ID, and (b) back-end tokenization. The virtual ID service uses front-end tokenization to allow users to keep their unique, 12-digit Aadhaar number hidden from service providers by generating a random, 16-digit virtual ID number. Once a user has generated a Virtual ID, they can provide that 16-digit number instead of their Aadhaar number for authentication. A key privacy-enhancing aspect is that the Virtual ID is temporary and revocable. In addition to virtual ID, UIDAI uses back-end tokenization to address the storage of Aadhaar numbers in service provider databases. Therefore, when a user gives their Aadhaar number or Virtual ID to a service provider for authentication, the system uses a cryptographic hash function to generate a 72-character alphanumeric token specific to that service-provider, which is stored instead of the full 12-digit Aadhaar number. Since different agencies receive different tokens for the same person, this prevents the linkability of information across databases.

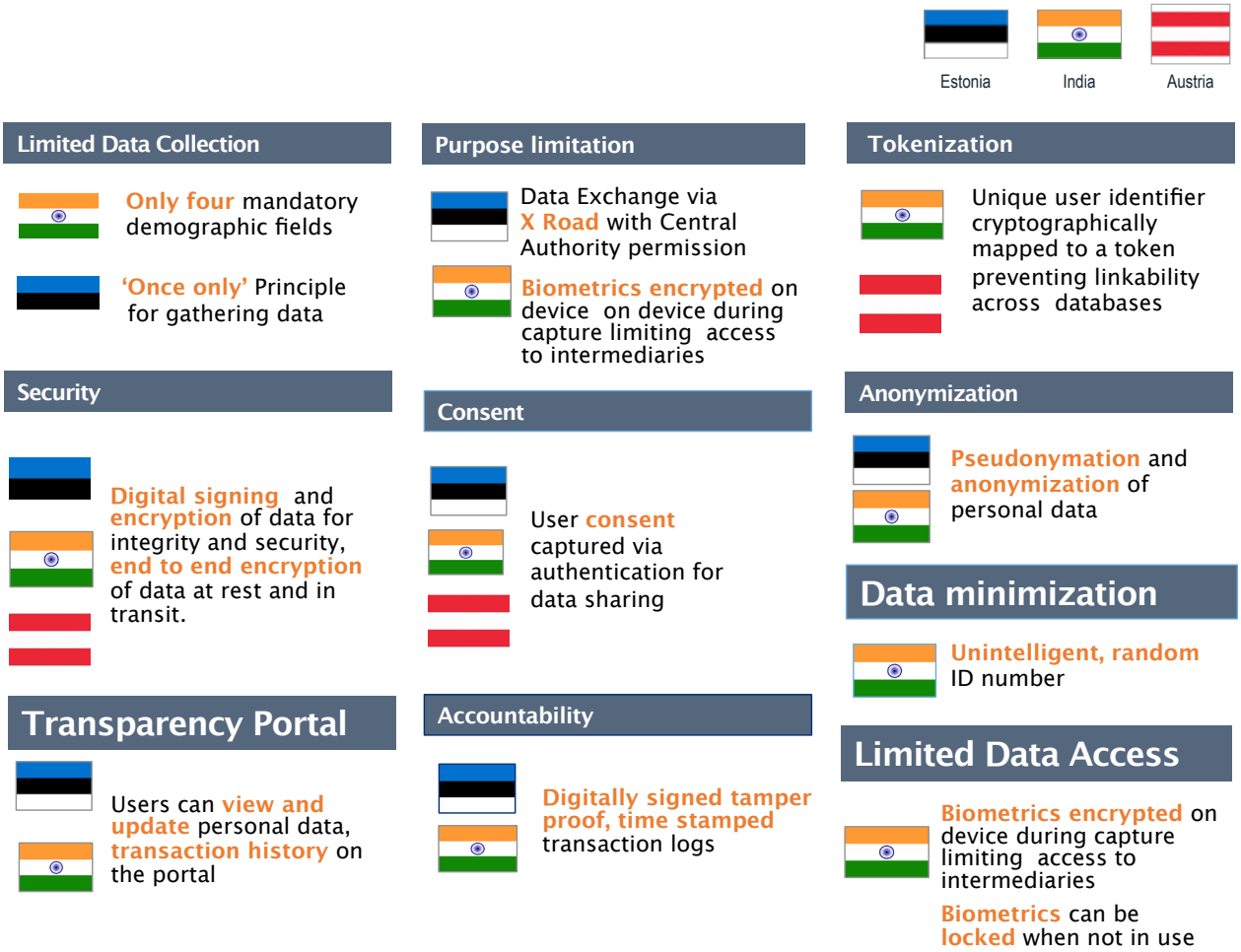
1. https://id4d.worldbank.org/research or http://documents.worldbank.org/curated/en/508291571358375350/pdf/Digital-ID-and-the-Data-Protection-Challenge-Practitioners-Note.pdf
2. https://id4d.worldbank.org/principles
3. First conceptualized by Ann Cavoukian as "Privacy by Design" or PbD. See Cavoukian, Ann. 2011. Privacy by Design. https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf
4. https://id4d.worldbank.org/research or http://documents.worldbank.org/curated/en/546691543847931842/pdf/Privacy-by-Design-Current-Practices-in-Estonia-India-and-Austria.pdf
5. https://github.com/e-gov/AJ

AUSTRIA – Example: Austria's Sector Specific Identifiers

Austria has taken multiple steps to limit linkability across databases. Rather than storing the 12-digit identifier (CRR number) on its virtual citizen card (CC) in plain form, it stores a "SourcePIN"—a unique identifier created by strong encryption of the CRR number. The data stored on the CC is signed by the SourcePIN Register Authority and is protected by a PIN. In addition, the eGovernment Act stipulates that different identifiers be used for each of the country's 26 public administration sectors. A sector-specific personal identifier (ssPIN) is created from the SourcePIN using a one-way derivation, a tokenization method through which a sector specific-pin is algorithmically computed from the SourcePIN. Public authorities can use the ssPIN to retrieve a citizen's data stored within the same sector, for example, if they need to view the citizen's records or use it to pre-fill forms.

More examples of PbD practices from each of the three countries are summarized in the image below, and more detail can be found in the full PbD report and ID4D Practitioner's Guide[6] on the ID4D website.

EXAMPLES PRIVACY BY DESIGN PRACTICES ACROSS THE GLOBE



6. https://id4d.worldbank.org/guide