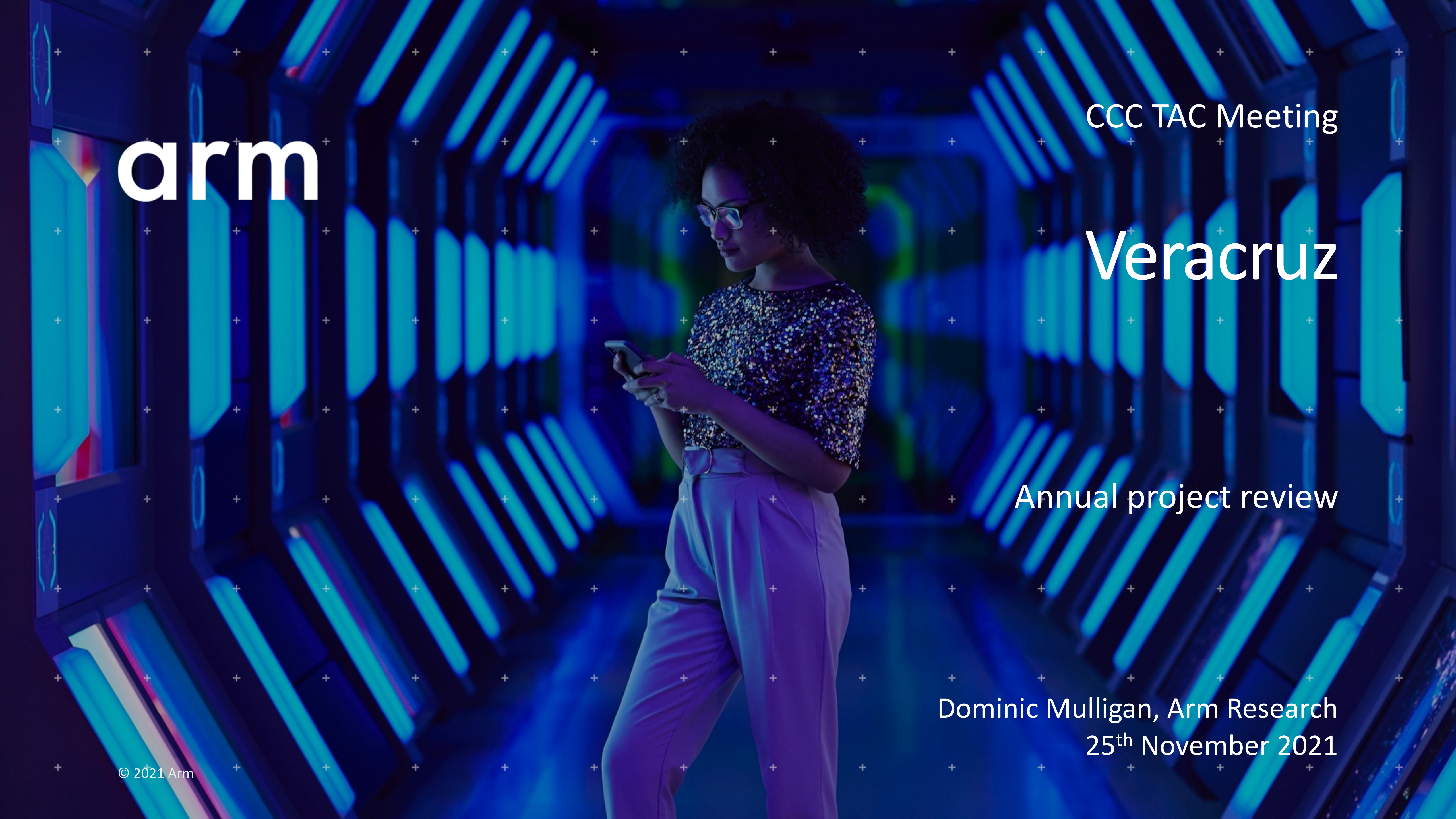


CCC TAC Meeting

# Veracruz

Annual project review

Dominic Mulligan, Arm Research
25th November 2021

arm

# Veracruz: privacy-preserving collaborative computation

https://github.com/veracruz-project/veracruz

# The Veracruz framework

## A framework for defining flexible and efficient multi-party computations

Veracruz aims to support common use-cases for advanced cryptographic techniques

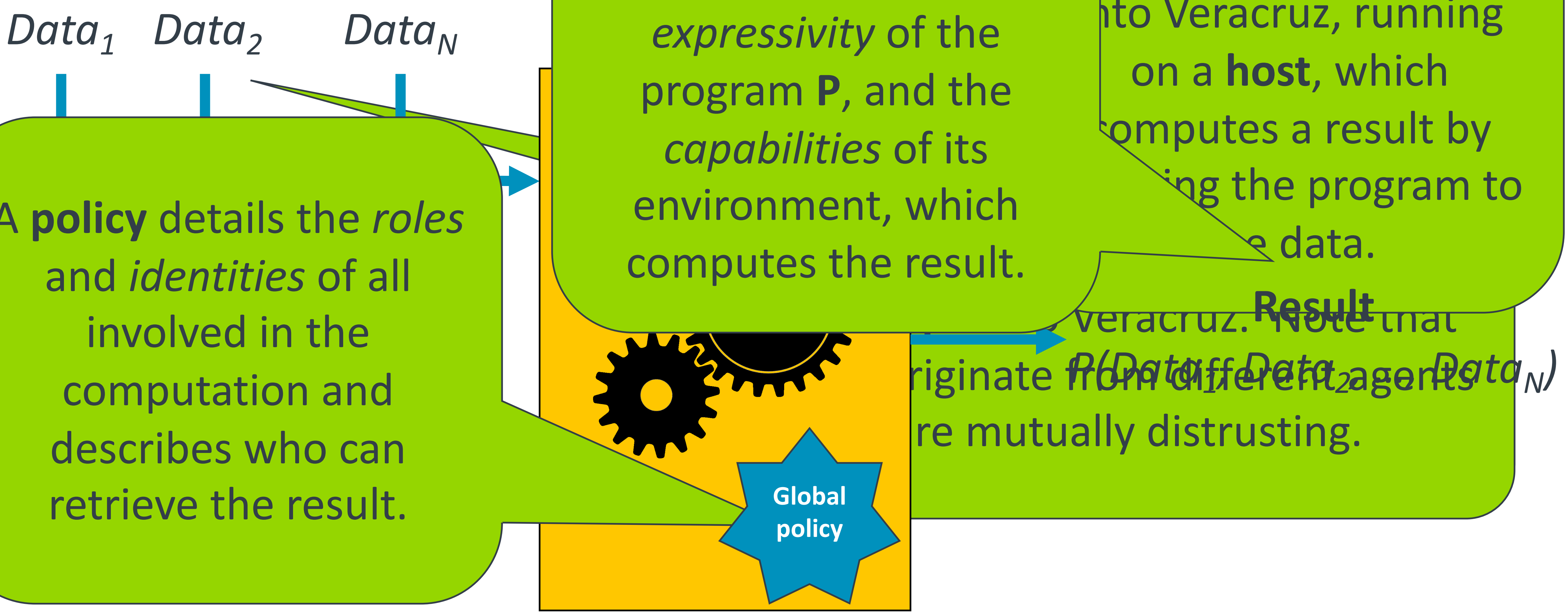
- Techniques like *homomorphic encryption*, *secure-multiparty computations,* and similar

Unlike those techniques, we aim to be:

1. **Efficient**: Be fast enough to execute ”interesting” programs,
2. **Familiar**: Allow programmers to use familiar programming languages and tools,
3. **General**: Seamlessly support a large class of multi-party computations,
4. **Reusable:** Provide a single framework supporting a wide-range of privacy-preserving computations without requiring significant reconfiguration for each task

In common with those techniques, we aim to provide a strong **security/privacy guarantee**

# Veracruz from 50,000ft



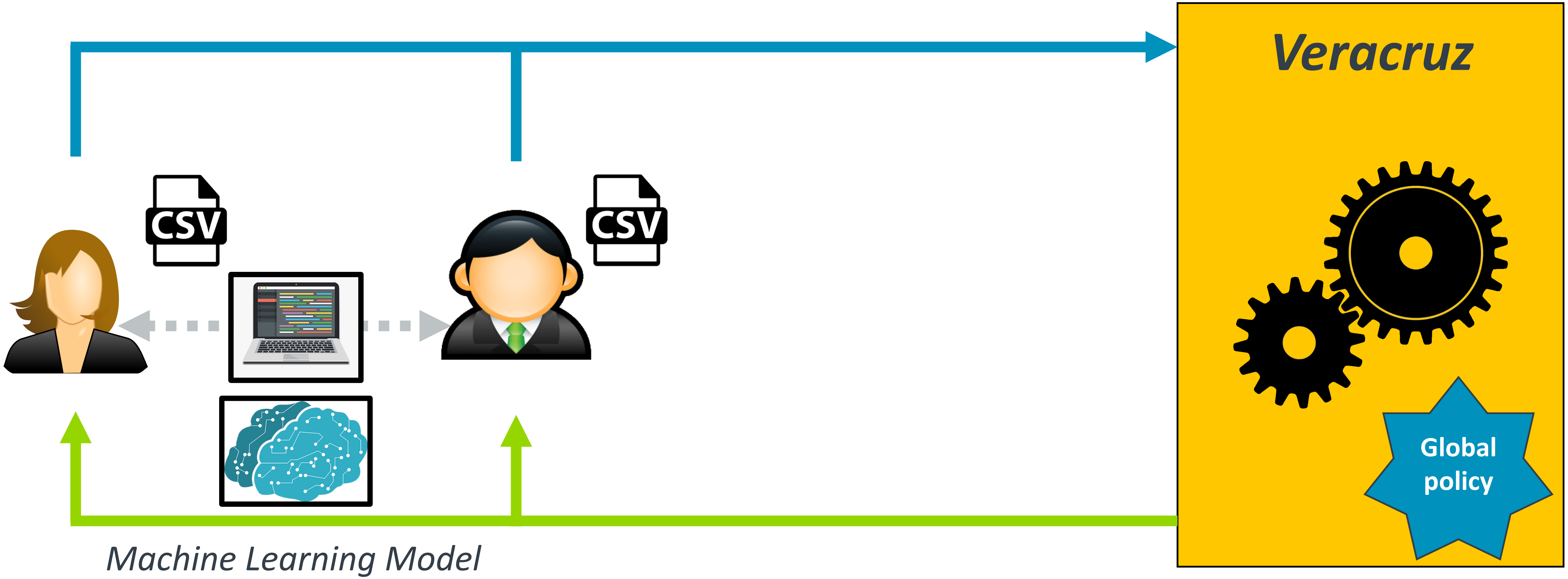
Program and data are provisioned securely nto Veracruz, running on a **host**, which omputes a result by ing the program to e data.

To maintain secrecy we need to control the *expressivity* of the program **P**, and the *capabilities* of its environment, which computes the result.

Veracruz. Note that riginate from different agents re mutually distrusting.

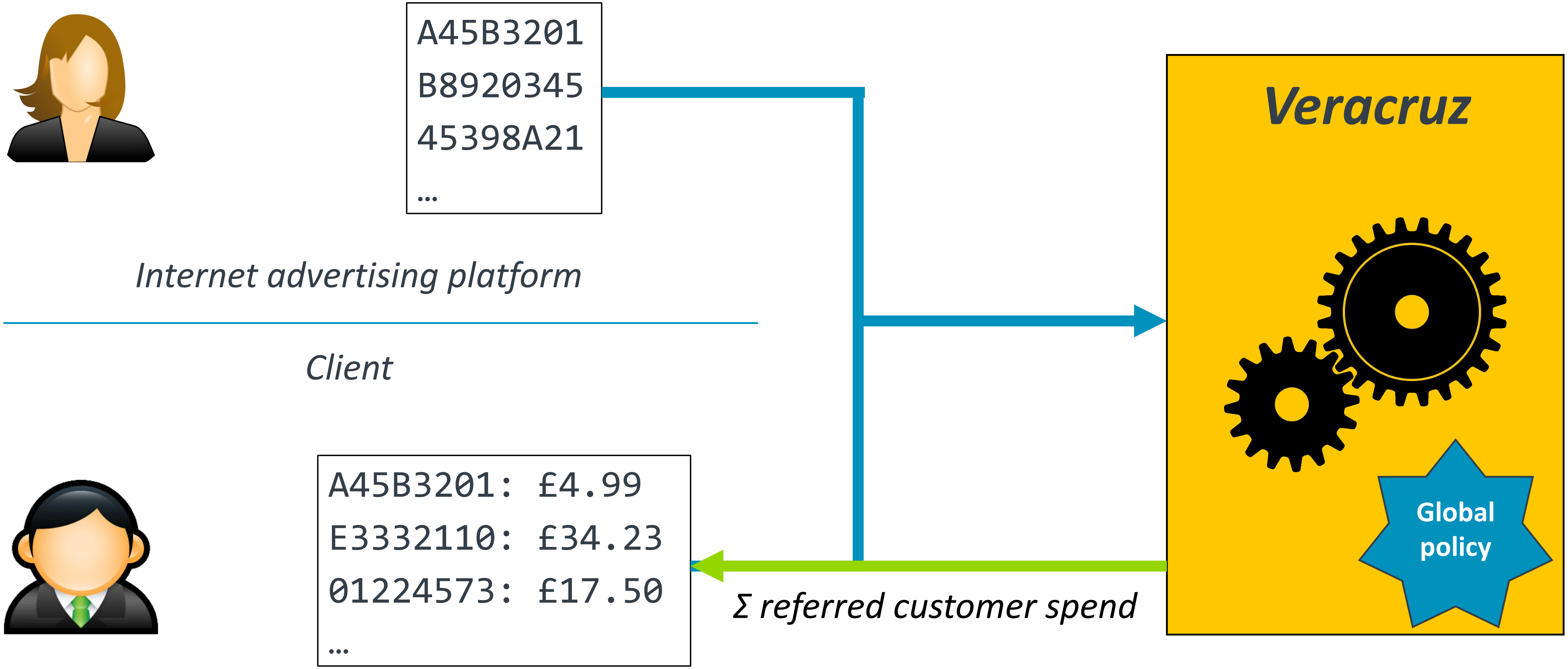
A **policy** details the *roles* and *identities* of all involved in the computation and describes who can retrieve the result.

# Use-case: privacy-preserving machine learning



*Machine Learning Model*

# Use-case: privacy-preserving set-sum computation



A45B3201
B8920345
45398A21
…

*Internet advertising platform*

*Client*

A45B3201: £4.99
E3332110: £34.23
01224573: £17.50
…

*Σ referred customer spend*

***Veracruz***

# …and many more potential use-cases

1. Privacy-preserving surveys/auctions/elections,
2. Privacy-preserving distributed compute: map-reduce/grid computing *a la* SETI@home,
3. Private search/fuzzy matching,
4. Provenance tracking for data,
5. Verifiable computation,
6. N-way secret sharing,
7. Fair exchange of documents,
8. IP protection,
9. Zero-knowledge proof of knowledge,
10. Delegating computations from weak devices to untrusted servers,

*…ad infinitum*

# Abstracting over isolates

Veracruz supports *multiple* different isolation technologies at present:

- **Arm TrustZone** trusted applications, and **Arm CCA** Realms (internally),
- **Intel SGX** secure enclaves,
- **AWS Nitro Enclaves**,
- The high-assurance **seL4 microkernel**, and plain **Linux** processes…

…representing different points on a *continuum of paranoia*

Veracruz provides abstractions over isolate technologies, with:

- A single, portable programming model based on **WebAssembly** and **WASI**
- A unified attestation mechanism, using **PKI**

Thank You

Danke

Gracias

谢谢

ありがとう

Asante

Merci

감사합니다

धन्यवाद

Kiitos

شكرًا

ধন্যবাদ

תודה

arm