



eCert: A User-Centric eCertificate System

Learning Societies Laboratory,
School of Electronic and Computer Science,
University of Southampton, UK

The Changing World of Security



- The “fortress” view of security
- But it was only last year that...
- The implications of peer to peer, linked data and our modern networked world

The Linked Data Problem



- It's amazing what data exists “out there”
- Modern systems (my 'phone!) can access it, link it... and lose it or abuse it
- The “club” entry scenario
- It would be great if I could regain control of my data

What the eCert project is all about



- We began with the problem of certificates in ePortfolios
- Computer scientists know about transaction processing
- But “eCertificates” are different
- We are investigating a good solution for ePortfolios and the broader scenarios

eCertificate Problems and Issues



Three stakeholder trust

Security requirements for satisfying the trust:

- Confidentiality, Privacy, Integrity, Authentication, Identity, Lifetime Validation.

The technical problems:

- Content validation of digitally signed document
- Auto request of validation
- The structural issues when applying digital signing

eCertificate System Goals



Maintain information privacy, ensure owner can have control over the usage of their eCertificates;

Prevent unauthorized modification, able to be verified in a legal context;

Lifetime validation, independent from issuing body. Allow for verification nationwide;

Easy to use while maintaining security controls, suit users with low IT skills, both students and reviewers;

Can be accessed through the issuing organizations, or any owner-preferred ePortfolio, or be used as a standalone application

How the eCert project works - 1



An eCertificate:

- Contains three sections, digitally signed, encrypted,
- With built-in functions to allow usage control settings while maintaining the integrity of the digital signature
- The status of the award, the signer and the signing key, expiry time, access time, and content modification, will all be validated

How the eCert project works - 2



The three stakeholders & the three subsystems

- Educational organization – create & issue
- Learner – manage & distribute
- Reviewer – view & verify

How the eCert project works - 3



The issuing subsystem is for registered educational organizations only

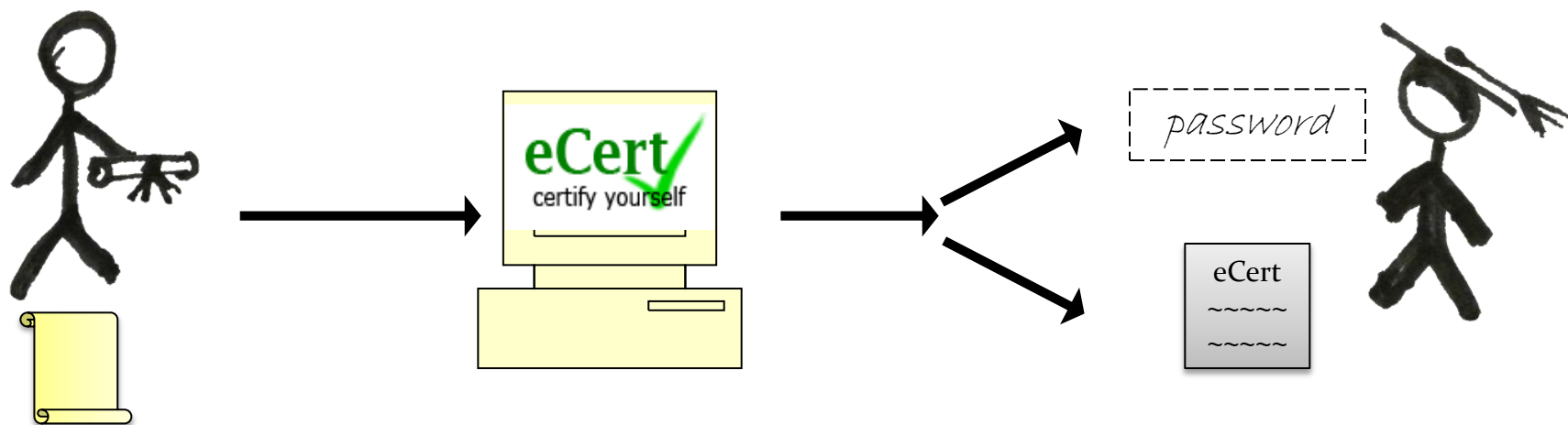
An eCert central system

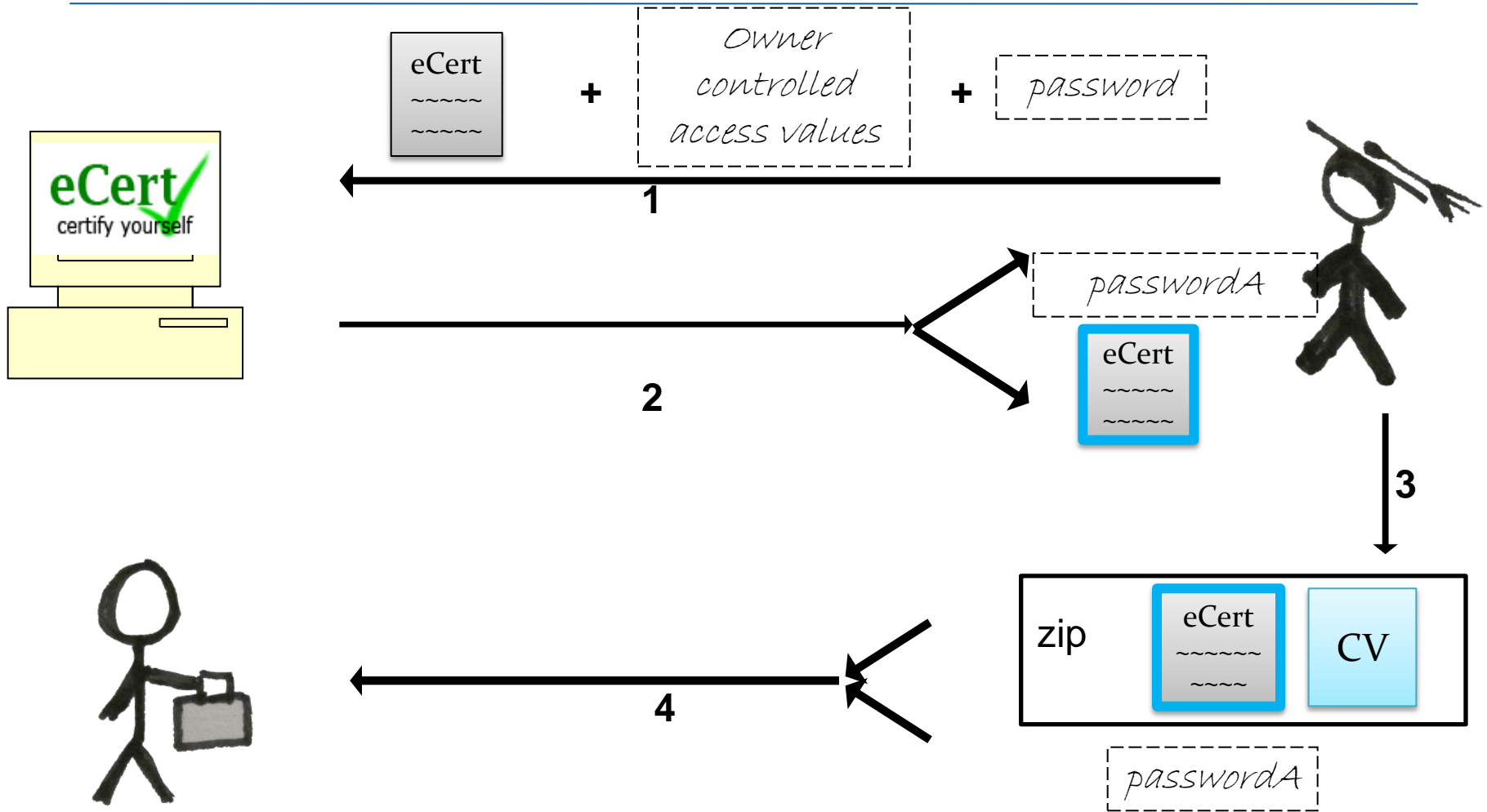
- Provides management and verification services
- No stored eCertificates – save storage, avoid attacks
- Convenient access
- Lifetime validation

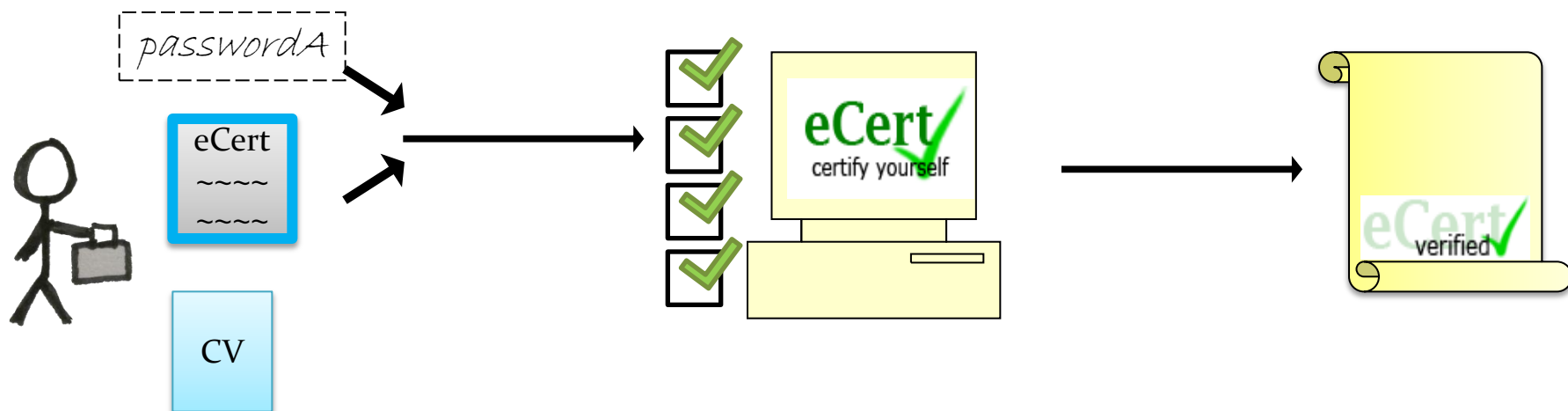
Example use cases



- CV with attached Maths A-Level certificate from Edexcel
- Evidence of work for a portfolio
- Sharing work with tutors, but securing access (i.e. for non-disclosure agreements)
- Many more....







eCert demonstration



- Educational organization → [issuing subsystem](#)
 - Issuing and sending the eCert to an eCert owner.
- Owner → [management subsystem](#)
 - Verifying the eCert, setting the access control to the eCert and sending it to a reviewer.
- Reviewer → [verification subsystem](#)
 - Verifying the eCert of an owner.

eCert in ePortfolio demonstration



- YouTube:

<http://www.youtube.com/watch?v=c9lc9vS3Eyg>

eCert for mobile eID demonstration



- (video)

What we have achieved (1)



- Code library implementing the eCert protocol
- A demonstrator showing how the code library can be used in ePortfolio systems
- A demonstration of eCert implemented in “eFolio”, Southampton's home-brewed ePortfolio system
- A demonstration of eCert implemented in Mahara (the Australian open-source ePortfolio system)
- A demonstration of eCert underpinning a mobile eID system, implemented as an Android app
- We're working on eCert implemented in Sharepoint

What we have achieved (2)



- All code is open source, located in Source Forge, and accessible from the eCert website
- All the demonstrators are also available via the project website, together with all the necessary documentation
- All reports, project documentation, and evaluations are also available via the project website

Thank you for coming



Questions?