JISC Completion Report

Project Document Cover Sheet

Project Information			
Project Acronym	Shintau		
Project Title	Shib-Grid Integrated Authorization		
Start Date	1 March 2007	**End Date**	31 July 2009
Lead Institution	University of Kent		
Project Director	Professor David Chadwick		
Project Manager & contact details	Professor David Chadwick University of Kent, Computing Laboratory, Canterbury, CT2 7NF. Email: d.w.chadwick@kent.ac.uk Mobile: +44 77 96 44 7184		
Partner Institutions	Internet 2		
Project Web URL	http://sec.cs.kent.ac.uk/shintau/		
Programme Name (and number)	e-Infrastructure (security)		
Programme Manager	Christopher Brown		

Document Name			
Document Title	**Completion Report**		
Reporting Period	*March 2007- July 2009*		
Author(s) & project role	D.W.Chadwick, Project Manager		
Date	29 May 2010	**Filename**	ShintauCompletionReport.doc
URL	http://sec.cs.kent.ac.uk/shintau/completionreport.pdf		
Access	☐ Project and JISC internal	✓ General dissemination	

Document History		
Version	**Date**	**Comments**
0.9	8 January 2010	Initial version
1.0	11 January 2010	Final version
1.01	29 May 2010	Additional financial figures inserted

JISC Completion Report

Project Sign-off

1. Project Outputs

The project deliverables, as specified in the original project proposal, are listed below in bold. The status of each one of them is then described.

D1.1 The SAMLv2 profile as Internet2 best practice or OGF specifications

We did not need a new SAMLv2 profile as it turned out, since we used Liberty Alliance WSF-IDF specifications. We did need to make a small change to the Liberty Alliance WSF-Discovery protocol, by adding a new Boolean Attribute to the discovery message (this tells the Linking Service whether it should perform the aggregation or leave it to the SP), and we have discussed with the LA group how this should be addressed. The conclusion of the LA group was that a new Discovery profile should be written which describes the purpose of this Boolean. However, these discussions took place after the Shintau project had completed, and under continuation funding from the EC TAS3 project, we have now devised a different protocol mapping which is much simpler than using the LA Discovery protocol, and requires less message exchanges. So we now propose to implement this new protocol mapping under funding from the TAS3 project. This should significantly increase the performance of attribute aggregation and be simpler to implement. (Part of the reason for looking for another protocol mapping was the complexity of installing the Shintau software, as reported by the University of Glasgow (NESC) in their usability trials. The new installation will not require the LA protocol stack to be installed.)

D1.2 A paper to an international conference describing the profiles to the research community.

We have comfortably exceeded this deliverable by publishing 3 journal papers and 1 conference paper, as detailed below.

1. George Inman, David Chadwick, Nate Klingenstein. “Authorisation using Attributes from Multiple Authorities – A Study of Requirements”. Presented at HCSIT Summit - ePortfolio International Conference,16-19 October 2007, Maastricht, The Netherlands.
2. David W Chadwick, George Inman. “Attribute Aggregation in Federated Identity Management”. IEEE Computer, May 2009, pp 46-53
3. David W. Chadwick, George Inman, Nate Klingenstein “A Conceptual Model for Attribute Aggregation”. Future Generation Computer Systems. Accepted Dec 2008. To be published in 2010.
4. George Inman, David Chadwick. “A Privacy Preserving Attribute Aggregation Model for Federated Identity Managements Systems”. Upgrade, Vol. IX, issue no. 6 (December 2009): "Privacy and Identity Management"

D2.1 The nAA-PIP that supports the push mode of attribute aggregation with optionally signed and encrypted SAML assertions
D3.1 The nAA-PIP that supports the pull mode of attribute aggregation.

This software has been incorporated into the standard PERMIS PDP/CVS software, as a new type of attribute repository, and it is callable via the PERMIS Java API by any application. The software is available as precompiled binaries from
http://sec.cs.kent.ac.uk/permis/downloads/Level2/decisionEngine.shtml

It is also available as part of a new standalone authorisation server which is called using either of the following OGF profiles:

1. David Chadwick, Linying Su. “Use of WS-TRUST and SAML to access a Credential Validation Service”. GFD.157. 13 November 2009. Available from http://www.ogf.org/documents/GFD.157.pdf
2. David W Chadwick, Linying Su, Romain Laborde. “Use of XACML Request Context to Obtain an Authorisation Decision”. GFD.159. 13 November 2009. Available from http://www.ogf.org/documents/GFD.159.pdf

This software is available as precompiled binaries from
http://sec.cs.kent.ac.uk/permis/downloads/Level3/standalone.shtml

All the software is available as open source code from www.openpermis.org and from our public SVN server at https://projects.kent.ac.uk/projects/permis/

D4.1 A modified mod_permis for Apache that picks up the collection of attributes and pushes them to the backend PERMIS nAA-PIP and PDP.

A modified mod_permis for Apache is not needed if the PERMIS SAAM software is used, since the attribute aggregation functionality is built into the backend PERMIS system. However, if the new standalone PERMIS authorisation server is used, the front end client software for Apache that talks the GFD.159 protocol is being provided by ZXID as part of the EC TAS3 project. Once this software is fully debugged and documented we will put a pointer to it on the PERMIS web site.

D5.1 An enhanced Globus Toolkit with a customizable nAA-PIP

No changes were needed to the GT software since the attribute aggregation functionality of the nAA-PIP has been built entirely into the PERMIS CVS software.

D7.1 A working demonstration of the nAA-PIP in a current Grid project that will retrieve attributes from at least 3 IdPs.

This demonstration has been provided by the NeSC at the University of Glasgow and the user guide for the demonstration can be found here:

http://sec.cs.kent.ac.uk/shintau/user-guide.pdf

User trials were performed with the demonstration system and the report of the user trials can be found here:

http://sec.cs.kent.ac.uk/shintau/user-trials.pdf

D8.1 The integrated software packaged with GT4, released as binaries and open source

See above for details of the software releases.

D8.2. User, developer and administrator documentation for the package including information needed for its support in a Shibboleth-enabled environment

Administrator documentation describing how to install and test each element of the Shintau architecture in a Shibboleth-enabled environment is available from

http://sec.cs.kent.ac.uk/shintau/ShintauInstallationGuide_0.4.pdf

Additional user documentation detailing how to use of the software which was written in conjunction with the user trials performed by the NeSC at the University of Glasgow and is available from

http://sec.cs.kent.ac.uk/shintau/user-guide.pdf

Developer documentation describing how the software was integrated into existing software and the classes used to do so is available from

http://sec.cs.kent.ac.uk/shintau/ShintauArchitectureDesign.pdf

Additional documentation for the standalone server is available here

http://sec.cs.kent.ac.uk/permis/documents/standalone-user-guideV1.2.pdf

D8.3 A paper for an international conference or journal publicizing the work

As described above, 3 journal papers and one conference paper have been produced so far. (Others can be expected in the future as the EC TAS3 project is continuing to fund this work).

D8.4 Final report to JISC

This was produced and delivered to JISC on 17 October 2009. The final report can now be found here

http://sec.cs.kent.ac.uk/shintau/finalreport.pdf

2. Intellectual Property Rights

We confirm that there are no IPR issues that prevent the project outputs from being made available to the teaching, learning, and research communities now that the project has ended.

We confirm that all necessary permissions for third-party IPR have been granted. The permission from IAIK to use their binaries, which are included in the PERMIS binary releases, for research and educational purposes, can be found here
http://sec.cs.kent.ac.uk/permis/essentials/permislicence.shtml.

The BSD-like license for all the PERMIS open source code is included in each source file.

3. Project Staff

Mr George Inman has worked on this project as a research assistant, and is also studying for a PhD on the research topic “Attribute Aggregation”. He is expected to complete his PhD in 2011. He will continue to work on attribute aggregation under the EC TAS3 project.

Dr Stijn Lievens has worked on this project as a senior research fellow and is continuing to work on PERMIS under the EC TAS3 project.

The staff who worked on this project at the NeSC, University of Glasgow were Dr John Watts supervised by Professor Richard Sinnott.

4. Dissemination Plan

1. Please see Section 1 for a full list of the published articles.

2. We have given 3 presentations at Terena meetings:

i) David Chadwick. Aggregation of Attributes from Different Authorities. Presented at TERENA EMC2 meeting,04-05 February 2008, Marseilles, France. See
http://www.terena.org/activities/tf-emc2/meetings/10/slides/Shintau-EMC2.pdf

ii) George Inman "Attribute Aggregation in Federated Identity Management" Presented at; Terena Networking Confrence 2009, 8-11 June 2009, Malaga, Spain. See
http://tnc2009.terena.org/schedule/presentations/show.php?pres_id=9

iii) George Inman, David Chadwick. Results of the Shintau Project presented at EMC2 meeting, Rome, 22 October 2009. See http://www.terena.org/activities/tf-emc2/meetings/14/ShintauAttAgg.ppt

We have given 2 presentations at Internet 2 meetings:

iv) David Chadwick "Aggregation of Attributes from Different Authorities - Proposed Protocols" Presented at; Spring 2008 Internet2 Member Meeting, see http://events.internet2.edu/speakers/speakers.php?go=people&id=2285

iv) David Chadwick "Attribute Aggregation" Presented at ;Spring 2009 Internet2 Member Meeting. See http://events.internet2.edu/2009/spring-mm/agenda.cfm?go=session&id=10000513&event=909

We have held one session at the 2009 Internet Identity Workshop, see

vi) http://iiw.idcommons.net/Attribute_Aggregation

3. We have liaised with the Liberty Alliance ID-WSF standard's group about the topic of attribute aggregation and are currently participating in two new Kantara Initiative working groups UMA and ID-WSF Evo to cover the topic of attribute aggregation

4. We have a project web site at http://sec.cs.kent.ac.uk/shintau/

5. We have a public hands-on demonstration of attribute aggregation available at http://issrg-beta.cs.kent.ac.uk:8080/loademo.html

5. Exit Plan

The University of Kent has several web sites for disseminating the project outputs as described above.

i) We confirm that the University of Kent will continue to host the Shintau project and PERMIS web sites for 3 years after the project end date and will assist JISC in archiving it subsequently.

In addition to the above, the SWISS Ministry of Defence has re-engineered and hardened the core of the PERMIS software and has made this publicly available at http://www.osor.eu/projects/openpermis. Since this software is being used in a military application, it is likely that the SWISS MoD will continue to support this version of PERMIS for the foreseeable future.

6. Sustainability Plan

Attribute aggregation (and other authorisation capabilities) are continuing to be developed by the University of Kent under the EC TAS3 project. The core of PERMIS has also been commercially hardened by the SWISS Ministry of Defence for a military application and this software is being published and maintained as open source software at OSOR web site.

Other commercial companies are using PERMIS and downloads are currently running at several hundred per month. It is likely that other initiatives will emerge in the coming months which will continue to sustain and further develop the PERMIS software suite.

7. Budget

The project did receive, and is continuing to receive, funds from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 216287 (TAS³ - Trusted Architecture for Securely Shared Services). This money is being used to continue the research in attribute aggregation (and other authorisation topics) and to fund the final two years of George Inman's PhD. Other authorisation features that are currently being added to PERMIS include: Support for Break the Glass policies, distributed support for enforcing obligations, multiple policy evaluation and policy conflict resolution.

Lessons Learned

8. Aims and Objectives

From the PI's perspective this project has been very successful. We have achieved all the project's original stated objectives and surpassed many of them, without needing to change any of them. We have working software which is publicly available as open source code for download and we have a demonstration system that is publicly available here:

http://issrg-beta.cs.kent.ac.uk:8080/loademo.html

We (with the invaluable help of the NeSC, Glasgow) have performed successful user trials, the report of which can be found here:

http://sec.cs.kent.ac.uk/shintau/user-trials.pdf

We are now in a position to modify the design and build the next generation system that will address the weaknesses in the current Shintau system as identified in the user trials i.e. complexity of installation, slow performance due to the number and complexity of the protocol messages that are involved, and no ability for users to dynamically select their attributes and provide consent for each one to be aggregated (only static aggregation is available in the current version with dynamic consent of linking). The installation report from NESC can be found here:

http://sec.cs.kent.ac.uk/shintau/installation-report.pdf

Since we have won additional funding from the EC to continue our research into authorisation (including privacy preserving attribute aggregation) we expect to be able to provide an enhanced version of the Shintau software during the next year. Attribute aggregation is an important topic that has still not yet been adequately addressed by anyone in the research or commercial identity management community, and we hope that the University of Kent will be the first to do this, primarily as a result of the JISC funding of the Shintau project.

9. Overall Approach

The only thing we would have done differently is to have increased the duration of the project, though not the overall cost. This is because the first half of the project, liaising with the user community to gather requirements, and liaising with the standards organisations to determine which protocol suite to use, took rather longer than anticipated, and resulted in us having to produce a second set of protocol mappings as a result of feedback from the Liberty Alliance group. Implementation then took as long as anticipated but started late, necessitating us to have to ask for a no-cost extension (which JISC graciously granted).

10. Project Outcomes

The main outcomes were reported in the final report and will not be repeated here. In addition to these, we have since performed a user trial and the main outcomes from this are:

- the Shintau software provides an effective solution to attribute aggregation
- it was found to be generally easy to use by the NeSC users, but they thought it would not be easy enough for non-expert users
- the UK Access Management Federation should consider supporting the Shintau infrastructure
- the NeSC users regarded gaining access to a service as being equally important as privacy protecting their attributes.

The only thing to add to the Final Report is that the University of Kent has been awarded the Logins for Life project and therefore will now be able to integrate the Shintau account Linking Service into a pilot operational Logins for Life service at the University of Kent. The impact of this is to allow closer links between the university and its associates (alumni, staff and future students).

11. Stakeholders

The likely beneficiaries are all users of the Internet who need to send an aggregated set of their attributes to a service provider, in order to receive an enhanced level of service, whilst maintaining their privacy. Service providers are also beneficiaries since it enables them to increase their trust in the user at the remote end of a communication and thereby reduce their risk in providing an enhanced level of service to him/her. This should reduce the incidence of fraud, improve user privacy, enable users to provide consent for their personal attributes to be released, increase trust and thereby reduce the overall cost of doing business over the Internet.

12. Project Partners

The NESC, University of Glasgow was a subcontractor to the University of Kent. The role of NESC was to take the Shintau developed software, install it, build a grid application that required attribute aggregation, and then test the application with a sample of grid users and report on the outcome. Kent provided appropriate help and support to NESC throughout this period and helped with the analysis of the results. The collaboration was successful and user results are very positive as described in the user trials report (URL given above). The two organisations, University of Kent and NESC, and their PIs, Professors Chadwick and Sinnott, have previously worked together successfully on several projects prior to Shintau, and therefore they already had a good working relationship. This is bound to have been a positive factor in this project, and is likely to be so in any future collaborations.

13. Project Management

Project management is always a critical success factor in any project. This project was no different. The project manager needs to continually monitor the progress of the project, and when deviations to the project plan arise, take the appropriate corrective action. When the project cannot be brought back on track, which happened in this project during the design stage and interaction with the standards community, then it is inevitable that the plan will need to change to take account of the delays. It is at this point that a sympathetic JISC programme manager is a major asset to project management.

14. Programme Support

Having a sympathetic programme manager, who granted the project a no-cost extension to its timescale, was a major asset whose benefit cannot be overstated. Without the extension we would not have been able to deliver the software to NESC in time, and NESC would not have been able to carry out the user trials.

15. Future Work

In the Conclusions and Recommendations section of the Final Report we listed a number of issues that need to be addressed by JISC, before attribute aggregation can become widely rolled out and accepted by the user community. JISC should pursue these now.

We also listed two different implementation options that could be funded as well as the issue of how attribute aggregation can be integrated into Microsoft's CardSpace. The University of Kent proposes to continue its research into attribute aggregation under the EC funded TAS3 project, and therefore further implementation funding by JISC is not required in the next 18 months. It remains to be seen what additional effort might be needed in 18 months time.

Appendix A. Final Budget

Directly Incurred Staff	**TOTAL BUDGET £**	**Year <07-08> Actual Expenditure**	**Year <08-09> Actual Expenditure**	**TOTAL EXPENDITURE £**	**TOTAL VARIANCE**
George Inman (Grade 7 pt32) @ 100%	£37,435	£21,216.96	£30,668.13	£51,885.09	£
Y Liang		£2,769.90	£3,396.20	£6,166.10	£
L. Su		£3,037.00	£8,777.71	£11,814.71	
S.F. Lievens (Grade 8 pt 37)		£ nil	£21,513.10	£21,513.10	
Software Engineer (G9pt44) @ 100%	£53,944	£	£	£	£
Total Directly Incurred Staff (A)	**£91,379**	**£**	**£**	**£91,379**	**£0**
Non-Staff					
Travel and expenses	£6,000.00	£3,806.43	£2,595.14	£6,401.57	£401.57
Hardware/software	£2,000.00	£ 500.00	£1,201.03	£1,701.03	£-298.97
Dissemination/Evaluation	£-	£-	£-	£-	£-
Consumables	£1,500.00	£ 28.70	£491.05	£519.75	£-980.25
Subcontracting	£30,000.00	£0	£29,763.43	£29,763.43	£-236.57
Total Directly Incurred Non-Staff (B)	**£39,500.00**	**£4,335.13**	**£34,050.65**	**£38,385.78**	**£-1,114.22**
Directly Incurred Total (A+B=C) (C)	**£130,879.00**	**£31,358.99**	**£98,405.79**	**£129,764.78**	**£-1,114.22**
Directly Allocated					
Staff (Prof Chadwick)	£25,049.00	£13,013.79	£13,102.13	£26,115.92	£1,066.92
Estates	£12,046.00	£6,023.00	£6,023.00	£12,046.00	£ nil
Directly Allocated Total (D)	**£37,095.00**	**£19,036.79**	**£19,125.13**	**£38,161.92**	**£1,066.92**

Indirect Costs (E)	**£60,791.00**	**£30,395.50**	**£30,395.50**	**£60,791.00**	**£nil**
Total Project Cost (C+D+E)	**£228,765.00**	**£80,791.28**	**£147,926.42**	**£228,717.70**	**£-47.30**
Funds Received from JISC	**£183,012.00**	**£23,762.00**	**£159,250.00**	**£183,012.00**	**£nil**
Institutional Contributions	**£45,753.00**	**£57,029.28**	**£-11,323.58**	**£45,705.70**	**£-47.30**

Nature of Institutional Contributions

Directly Incurred Staff					
George Inman (Grade 7 pt32) @ 100%	£10,368.43				
Y Liang	£1,232.20				
L. Su	£2,360.99				
S.F. Lievens (Grade 8 pt 37)	£4,299.06	£	£	£	£
Directly Incurred Non Staff					
Travel and expenses	£1,279.25				
Hardware/software	£339.92				
Consumables	£103.86				
Subcontracting (NESC)	£5,947.76	£	£	£	£
Directly Allocated					
Staff (Prof Chadwick)	£5,218.86	£	£	£	£
Estates	£2,407.21				
Indirect Costs					
Indirect Costs	£12,148.14	£	£	£	£
Total Institutional Contributions	**£45,705.70**	**£**	**£**	**£**	**£**