1506
UNIVERSITÀ
DEGLI STUDI
DI URBINO
CARLO BO

Via Aurelio Saffi, 2 – 61029 Urbino (PU)
Tel. +39 0722 3051
www.uniurb.it

SELEZIONE, PER ESAMI, FINALIZZATA ALL'ASSUNZIONE CON CONTRATTO DI LAVORO SUBORDINATO A TEMPO INDETERMINATO E PIENO DI **N. 1 UNITA' DI PERSONALE TECNICO-AMMINISTRATIVO DI CATEGORIA EP - AREA TECNICA, TECNICO-SCIENTIFICA ED ELABORAZIONE DATI** – PER LE ESIGENZE DEL **SERVIZIO SISTEMA INFORMATICO D'ATENEO**, **RISERVATO AL PERSONALE IN SERVIZIO A TEMPO INDETERMINATO PRESSO L'UNIVERSITÀ DEGLI STUDI DI URBINO CARLO BO,** AI SENSI DELL'ART. 52 COMMA 1-bis DEL D.LGS N. 165/2001. (D.D.G. n. 476 del 3 novembre 2020)

Comunicazione ai sensi dell'art. 19 del D. Lgs n. 33/2013 e s.m.i.

La Commissione giudicatrice, nominata con Decreto del Direttore Generale n. 3 dell'8 gennaio 2021, risulta così composta:

- Prof. Laerte SORINI	- Professore di II fascia – SECS-S/06 Metodi matematici dell'economia e delle scienze attuariali e finanziarie Università degli Studi di Urbino Carlo Bo Presidente;
- Prof.ssa Roberta BOCCONCELLI	- Professore di II fascia – SECS-P/08 Economia e gestione delle imprese Università degli Studi di Urbino Carlo Bo Componente;
- Ing. Luca CIARLATANI	- Esperto in Progettazione di Sistemi informatici Componente;
- Sig.ra Manola DI LUCA	- Cat. C – Area amministrativa Università degli Studi di Urbino Carlo Bo Segretaria.

comunica **le tracce delle prove scritte e delle prove orali predisposte:**

PROVE SCRITTE

<u>Prima Prova scritta</u>

PROVA N.2 (prova sorteggiata)

1. Il candidato descriva Shibboleth e il suo funzionamento.
2. Acquisizione software per la pubblica amministrazione: fasi e regole.

PROVA N. 1

1. Indicare e spiegare una strategia di backup.
2. Il candidato illustri come organizzerebbe lo smart working nella pubblica amministrazione con particolare riferimento ad una università di medie dimensioni.

PROVA N. 3

1. Il candidato descriva la configurazione di un cluster di un'applicazione web php/mysql.

2. Il candidato descriva le principali differenze tra IAAS, PAAS e SAAS.

Seconda Prova scritta

PROVA N. 2 (prova sorteggiata)

1. Il candidato illustri come integrerebbe il sistema di autenticazione SPID (Sistema Pubblico di Identità Digitale) con quello già esistente in Ateneo basato su Shibboleth.
2. Che cosa è un SIEM (Security Information and Event Management)?

PROVA N. 1

1. Che cosa si intende per "riuso del software" nella pubblica amministrazione?
2. Il candidato descriva le principali fasi di sviluppo di un sistema wireless per un ateneo, tenendo conto delle diverse tipologie di utenti.

PROVA N. 3

1. Che cosa è il disaster recovery e come può essere implementato in un ateneo?
2. Quali sono i vantaggi e gli svantaggi delle strategie di "make" e di "buy" di un software?

PROVE ORALI

PROVA N. 2 (prova sorteggiata)

1 Considerando il periodo che stiamo vivendo le amministrazioni si sono avvalse maggiormente dello Smart Working. Il candidato illustri quali possono essere i vantaggi e gli svantaggi di tale modalità e le eventuali criticità della sua messa in opera.

2 Il candidato illustri le tecniche di gestione e monitoraggio di una rete wireless per un ateneo evidenziandone i vantaggi e le criticità.

3 Prova di Lingua inglese - Leggere e tradurre

Shibboleth: Single Sign-on architecture

Shibboleth is a single sign-on log-in system for computer networks and the Internet. It allows people to sign in using just one identity to various systems run by federations of different organizations or institutions. The federations are often universities or public service organizations. The Shibboleth Internet2 middleware initiative created an architecture and open-source implementation for identity management and federated identity-based authentication and authorization (or access control) infrastructure based on Security Assertion Markup Language (SAML). Federated identity allows the sharing of information about users from one security domain to the other organizations in a federation. This allows for cross-domain single sign-on and removes the need for content providers to maintain user names and passwords. Identity providers (IdPs) supply user information, while service providers (SPs) consume this information and give access to secure content.

Shibboleth: Architecture

Shibboleth is a web-based technology that implements the HTTP/POST artifact and attribute push profiles of SAML, including both Identity Provider (IdP) and Service Provider (SP) components. Shibboleth 1.3 has its own technical overview, architectural document, and conformance document that build on top of the SAML 1.1 specifications. In the canonical use case:

- A user first accesses a resource hosted by a web server (the service provider) that has Shibboleth content protection enabled.
- The SP crafts a proprietary authentication request that is passed through the browser using URL query parameters to supply the requester's SAML entityID, the assertion consumption location, and optionally the end page to return the user to.
- The user is redirected to either their home IdP or a WAYF (Where Are You From) service, where they select their home IdP for further redirection.
- The user authenticates to an access control mechanism external to Shibboleth.
- Shibboleth generates a SAML 1.1 authentication assertion with a temporary "handle" contained within it. This handle allows the IdP to recognize a request about a particular browser user as corresponding to the principal that authenticated earlier.
- The user is POSTed to the assertion consumer service of the SP. The SP consumes the assertion and issues an AttributeQuery to the IdP's attribute service for attributes about that user, which may or may not include the user's identity.
- The IdP sends an attribute assertion containing trusted information about the user to the SP.
- The SP either makes an access control decision based on the attributes or supplies information to applications to make decisions themselves.

Shibboleth supports a number of variations on this base case, including portal-style flows whereby the IdP mints an unsolicited assertion to be delivered in the initial access to the SP, and lazy session initiation, which allows an application to trigger content protection through a method of its choice as required. Shibboleth 1.3 and earlier do not provide a built-in authentication mechanism, but any Web-based authentication mechanism can be used to supply user data for Shibboleth to use. Common systems for this purpose include CAS or Pubcookie. The authentication and single-sign-on features of the Java container in which the IdP runs (Tomcat, for example) can also be used. Shibboleth 2.0 builds on SAML 2.0 standards. The IdP in Shibboleth 2.0 has to do additional processing in order to support passive and forced authentication requests in SAML 2.0. The SP can request a specific method of authentication from the IdP. Shibboleth 2.0 supports additional encryption capacity.

PROVA N. 1

1 Il candidato illustri le diverse modalità di approccio al software in termini di riuso, fabbricazione e acquisto per una pubblica amministrazione evidenziando le criticità e i vantaggi per ogni scelta
2 Il candidato illustri le tecniche per la messa in sicurezza dei dati informatici all'interno di un ateneo.
3 Prova di Lingua inglese - Leggere e tradurre

Shibboleth: Single Sign-on architecture

Shibboleth is a single sign-on log-in system for computer networks and the Internet. It allows people to sign in using just one identity to various systems run by federations of different organizations or institutions. The federations are often universities or public service organizations. The Shibboleth Internet2 middleware initiative created an architecture and open-source implementation for identity management and federated identity-based authentication and authorization (or access control) infrastructure based on Security Assertion Markup Language (SAML). Federated identity allows the sharing of information about users from one security domain to the other organizations in a federation. This allows for cross-

domain single sign-on and removes the need for content providers to maintain user names and passwords. Identity providers (IdPs) supply user information, while service providers (SPs) consume this information and give access to secure content.

Shibboleth: History

The Shibboleth project grew out of Internet2. Today, the project is managed by the Shibboleth Consortium. Two of the most popular software components managed by the Shibboleth Consortium are the Shibboleth Identity Provider and the Shibboleth Service Provider, both of which are implementations of SAML. The project was named after an identifying passphrase used in the Bible (Judges 12:4–6) because Ephraimites were not able to pronounce "sh". The Shibboleth project was started in 2000 to facilitate the sharing of resources between organizations with incompatible authentication and authorization infrastructures. Architectural work was performed for over a year prior to any software development. After development and testing, Shibboleth IdP 1.0 was released in July 2003. This was followed by the release of Shibboleth IdP 1.3 in August 2005. Version 2.0 of the Shibboleth software was a major upgrade released in March 2008. It included both IdP and SP components, but, more importantly, Shibboleth 2.0 supported SAML 2.0. The Shibboleth and SAML protocols were developed during the same timeframe. From the beginning, Shibboleth was based on SAML, but, where SAML was found lacking, Shibboleth improvised, and the Shibboleth developers implemented features that compensated for missing features in SAML 1.1. Some of these features were later incorporated into SAML 2.0, and, in that sense, Shibboleth contributed to the evolution of the SAML protocol. Perhaps the most important contributed feature was the legacy Shibboleth AuthnRequest protocol. Since the SAML 1.1 protocol was inherently an IdP-first protocol, Shibboleth invented a simple HTTP-based authentication request protocol that turned SAML 1.1 into an SP-first protocol. This protocol was first implemented in Shibboleth IdP 1.0 and later refined in Shibboleth IdP 1.3. Building on that early work, the Liberty Alliance introduced a fully expanded AuthnRequest protocol into the Liberty Identity Federation Framework. Eventually, Liberty ID-FF 1.2 was contributed to OASIS, which formed the basis for the OASIS SAML 2.0 Standard.

Urbino, 22 gennaio 2021

LA COMMISSIONE GIUDICATRICE

- F.to Prof. Laerte SORINI (Presidente)

- F.to Prof.ssa Roberta BOCCONCELLI (Componente)

- F.to Ing. Luca CIARLATANI (Componente)

- F.to Sig.ra Manola DI LUCA (Segretaria)