ANX-PR/CL/001-01
GUÍA DE APRENDIZAJE

ASIGNATURA

613000044 - Aplicaciones para smartcards

PLAN DE ESTUDIOS

61AC - Master Universitario En Software De Sistemas Distribuidos Y Empotrados

CURSO ACADÉMICO Y SEMESTRE

2018/19 - Segundo semestre

Índice

Guía de Aprendizaje

1. Datos descriptivos

1.1. Datos de la asignatura

Nombre de la asignatura	613000044 - Aplicaciones para smartcards
No de créditos	3 ECTS
Carácter	Obligatoria
Curso	Primer curso
Semestre	Segundo semestre
Período de impartición	Febrero-Junio
Idioma de impartición	Castellano
Titulación	61AC - Master universitario en software de sistemas distribuidos y empotrados
Centro responsable de la titulación	61 - Escuela Tecnica Superior de Ingenieria de Sistemas Informaticos
Curso académico	2018-19

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Javier Garcia Martin (Coordinador/a)	4419	javier.garciam@upm.es	M - 19:00 - 21:00 J - 10:00 - 14:00

* Las horas de tutoría son orientativas y pueden sufrir modificaciones. Se deberá confirmar los horarios de tutorías con el profesorado.

3. Conocimientos previos recomendados

3.1. Asignaturas previas que se recomienda haber cursado

El plan de estudios Master Universitario en Software de Sistemas Distribuidos y Empotrados no tiene definidas asignaturas previas recomendadas para esta asignatura.

3.2. Otros conocimientos previos recomendados para cursar la asignatura

- Conocimientos de criptografía a nivel de usuario

4. Competencias y resultados de aprendizaje

4.1. Competencias

CG10 - Resolución de problemas.

CG11 - Razonamiento crítico.

4.2. Resultados del aprendizaje

RA87 - Trabajando en equipo, propone y construye soluciones a problemas en diferentes campos desde una perspectiva global.

RA31 - RA3_1 Identifica y conoce los protocolos de transmisión. RA3_2 Identifica y conoce los objetos de datos para distintas funciones. RA3_3 Conoce los procedimientos de transmisión de datos segura. Configura aplicaciones que usan métodos de autenticación, tarificación y almacenamiento de datos confidenciales orientados a smartcard.

RA33 - RA5_1 Conoce los comandos software orientados al desarrollo de aplicaciones y proyectos con smartcard.

RA34 - RA6_1 Conoce y maneja los tipos y las estructuras de ficheros de las tarjetas inteligentes. RA6_2 Conoce y maneja los sistemas operativos para tarjetas.

RA29 - RA1_1 Identifica, comprende y analiza los tipos y estructuras básicas para smartcard. RA1_2 Identifica, comprende y analiza los protocolos para smartcard. RA1_3 Identifica, comprende y analiza las tecnologías para comunicaciones con tarjetas

RA32 - RA4_1 Identifica y conoce las normas ISO para tarjetas de distinto campo. RA4_2 Conoce y comprende la interfaz y los protocolos de activación para tarjetas sin contacto RA4_3 Identifica y conoce los dispositivos NFC, sus protocolos y aplicaciones.

RA35 - RA7_1 Conoce y maneja estructuras para aplicaciones para sistemas de pago. RA7_2 Conoce y maneja estructuras para aplicaciones para sistemas de telecomunicación. RA7_3 Conoce y maneja estructuras para aplicaciones para identificación y gestión administrativa. RA7_4 Conoce y maneja estructuras para aplicaciones de carácter general.

RA30 - RA2_1 Entiende y aplica los diferentes sistemas de cifrado. RA2_2 Entiende y aplica estructuras PKI RA2_3 Conoce, comprende y configura mecanismos de autenticación y seguridad en dispositivos smartcard.

RA52 - Conoce y diseña aplicaciones para smarcard. Configura aplicaciones que utilizan smarcard para aplicaciones de autentificación, tarificación y almacenamiento de datos confidenciales.

RA88 - Realiza juicios y toma decisioness de forma razonada.Analiza, interpreta y evalúa información y argumentos desde distintos puntos de vista.Sintetiza y relaciona información y saca conclusiones de forma razonada.

5. Descripción de la asignatura y temario

5.1. Descripción de la asignatura

No hay descripción de la asignatura.

5.2. Temario de la asignatura

1. Introducción.
   - 1.1. 1.- Tipos de Tarjetas. Propiedades físicas y eléctricas. Tarjetas de contacto. Tarjetas sin contacto.
   - 1.2. 2.- Tipos de tarjetas de contacto atendiendo a su estructura.
   - 1.3. 3.-Terminales para smartcards. Seguridad. PCSC
2. Fundamentos de Criptografía, autentificación, aleatorios, estructuras de datos y corrección de errores (CRC).
   - 2.1. 1.- Funciones HASH, funciones PRF. Criptografía simétrica y asimétrica. Tipos de cifrado: DES, 3DES, AES. RSA.
   - 2.2. 2.- Certificados de claves publicas X509. PKI?s. Modos de funcionamiento de los cifradores.
   - 2.3. 3.- Firma digital

2.4. 4.- Generación de aleatorios. Aleatorios en tarjetas. Gestión de claves en las tarjetas.

2.5. 5.- Sistemas y métodos de Autenticación.

2.6. 6.- Estructuras de datos para tarjetas. Codificación de datos alfanuméricos. Códigos de detección de errores.

3. Comunicaciones con tarjetas con contacto.

3.1. 1.- Modelo de arquitectura en capas.

3.2. 2.- Tarjetas de contacto: Tipos, normativa, capa física.

3.3. 3.- Protocolos ISO de transmisión. Protocolos y comandos para comunicación con smartcard.

3.4. 4.- Objetos de datos para texto plano, para mecanismos de seguridad y para funciones auxiliares.

3.5. 5.- Transmisión de datos segura: Procedimiento de autentificación. Procedimiento combinado. Envío del contador de secuencia. Canales lógicos

4. Comunicaciones con tarjetas sin contacto.

4.1. 1.- Acoplamiento inductivo

4.2. 2.- Tarjetas de campo cercano (ISO/IEC 10536).

4.3. 3.- Tarjetas de campo próximo (ISO/IEC 14443).

4.4. 4.- Interfaz de comunicación. Tipos. Inicialización y anticolisión.Protocolos de activación para tarjetas tipo A. Desactivación

4.5. 5.- Tarjetas de campo medio (ISO/IEC 15693).

4.6. 6.- Dispositivos NFC. Protocolo NFC. Aplicaciones.

5. Comandos para tarjetas inteligentes.

5.1. 1.- Comandos básicos: selección, lectura, escritura, manipulación, y gestión de ficheros.

5.2. 2.- Comandos de identificación, autentificación y para uso con algoritmos criptográficos.

5.3. 3.- Comandos de gestión de aplicaciones

5.4. 4.- Comandos para la prueba del hardware.

5.5. 5.- Comandos para protocolos de transmisión de datos.

5.6. 6.- Comandos para bases de datos: SCQL.

5.7. 7.- Comandos para operaciones de pago: monederos electrónicos, tarjetas de crédito y débito.

6. Ficheros en tarjetas inteligentes.

6.1. 1.- Ficheros: Tipos, denominación y ciclo de vida.

6.2. 2.- Estructura del árbol de directorios.

6.3. 3.-Nombres de ficheros. FID. SFI.

6.4. 4.-Clasificación de ficheros atendiendo a su estructura interna.

6.5. 5.- Gestión de ficheros. Condiciones de control de acceso a ficheros. Atributos de los ficheros

6.6. 6.- Sistemas operativos para tarjetas. Javacards.

7. Aplicaciones de las Smartcards.

7.1. 1.- Tarjetas en sistemas de pago: prepago, débito, crédito. Monederos electrónicos. La aplicación EMV.

7.2. 2.- Tarjetas en sistemas de telecomunicación. El sistema GSM.

7.3. 3.- Entornos orientados a uso de aplicaciones para identificación personal y pasaportes.

7.4. 4.- Tarjetas criptográficas para autentificación y firma electrónica.

7.5. 5.- Entornos orientados a uso de otras aplicaciones: sistemas de transporte, sistemas de salud.

6. Cronograma

6.1. Cronograma de la asignatura *

Sem	Actividad presencial en aula	Actividad presencial en laboratorio	Otra actividad presencial	Actividades de evaluación
1	**Tema 1-Introducción.** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Realización de actividades prácticas** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	**Resolución de supuestos prácticos.** Duración: 03:00 PL: Actividad del tipo Prácticas de Laboratorio	**Resolución de programas, puesta en funcionamiento y pruebas. (RA29,RA30,RA31,RA32,RA87,RA88)** TI: Técnica del tipo Trabajo Individual Evaluación continua Duración: 03:00
2	**Tema 1-Introducción.** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Realización de actividades prácticas** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	**Resolución de supuestos prácticos.** Duración: 03:00 PL: Actividad del tipo Prácticas de Laboratorio	**Resolución de programas, puesta en funcionamiento y pruebas.(RA33,RA34,RA35)** TI: Técnica del tipo Trabajo Individual Evaluación continua Duración: 03:00
3	**Tema 1-Introducción.** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Realización de actividades prácticas** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio	**Resolución de supuestos prácticos.** Duración: 03:00 PL: Actividad del tipo Prácticas de Laboratorio	**Resolución de programas, puesta en funcionamiento y pruebas.(RA52,RA87,RA88)** TI: Técnica del tipo Trabajo Individual Evaluación continua Duración: 03:00
4				**Prueba de evaluación final ejercicios prácticos. (RA29,RA30,RA31,RA32,RA33, RA34,RA35,RA52,RA87,RA88)** EP: Técnica del tipo Examen de Prácticas Evaluación sólo prueba final Duración: 03:00 **Prueba de evaluación final ejercicios prácticos. (RA29,RA30,RA31,RA32,RA33, RA34,RA35,RA52,RA87,RA88)** EP: Técnica del tipo Examen de Prácticas Evaluación sólo prueba final Duración: 03:00
5				
6				
7				
8				
9				
10				
11				
12				
13				

14				
15				
16				
17				

Las horas de actividades formativas no presenciales son aquellas que el estudiante debe dedicar al estudio o al trabajo personal.

Para el cálculo de los valores totales, se estima que por cada crédito ECTS el alumno dedicará dependiendo del plan de estudios, entre 26 y 27 horas de trabajo presencial y no presencial.

* El cronograma sigue una planificación teórica de la asignatura y puede sufrir modificaciones durante el curso.

7. Actividades y criterios de evaluación

7.1. Actividades de evaluación de la asignatura

7.1.1. Evaluación continua

Sem.	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
1	Resolución de programas, puesta en funcionamiento y pruebas. (RA29,RA30,RA31,RA32,RA87,RA88)	TI: Técnica del tipo Trabajo Individual	Presencial	03:00	25%	5 / 10	CG10 CG11
2	Resolución de programas, puesta en funcionamiento y pruebas.(RA33,RA34,RA35)	TI: Técnica del tipo Trabajo Individual	Presencial	03:00	35%	5 / 10	CG10 CG11
3	Resolución de programas, puesta en funcionamiento y pruebas.(RA52,RA87,RA88)	TI: Técnica del tipo Trabajo Individual	Presencial	03:00	40%	5 / 10	CG10 CG11

7.1.2. Evaluación sólo prueba final

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
4	Prueba de evaluación final ejercicios prácticos. (RA29,RA30,RA31,RA32,RA33,RA34,RA35,RA52,RA87,RA88)	EP: Técnica del tipo Examen de Prácticas	No Presencial	03:00	50%	5 / 10	CG10 CG11
4	Prueba de evaluación final ejercicios prácticos. (RA29,RA30,RA31,RA32,RA33,RA34,RA35,RA52,RA87,RA88)	EP: Técnica del tipo Examen de Prácticas	No Presencial	03:00	50%	5 / 10	CG10 CG11

7.1.3. Evaluación convocatoria extraordinaria

No se ha definido la evaluación extraordinaria.

7.2. Criterios de evaluación

EVALUACIÓN CONTÍNUA:

La calificación final corresponderá a la suma de las calificaciones obtenidas por el alumno en la realización de los programas de todas

y cada una de las tareas a realizar en cada tema. Para que la evaluación sea continua hay que cumplir los siguientes

requisitos:

Haber entregado en tiempo y forma el 100% de las tareas establecidas.

Haber asistido con regularidad (al menos al 80%) de las clases presenciales.

En caso contrario el alumno deberá realizar un examen final teórico-práctico que incluirá todos los contenidos de la asignatura.

El examen se realizará en la siguiente convocatoria, a aquella en la que ha seguido la evaluación continua.

EVALUACIÓN mediante SOLO EXAMEN FINAL:

Los alumnos que deseen ser evaluados SOLO mediante examen final y no seguir la evaluación continua, deberán solicitarlo, por

escrito, antes de que finalicze la segunda semana de clase. Una vez finalizado el plazo no se admitirán peticiones excepto por

motivos de enfermedad y justificada con certificado médico.

El examen final consistirá en una prueba tipo examen teórico-prácticoque se calificará sobre 10 puntos, siendo necesario

obtener una nota igual o superior a 5 para superar la asignatura.

8. Recursos didácticos

8.1. Recursos didácticos de la asignatura

Nombre	Tipo	Observaciones
Diapositivas	Bibliografía	Colección de diapositivas realizadas por el profesor para cada tema.
Enlaces	Recursos web	Enlaces web a páginas con documentación aplicable a cada parte de los contenidos.
Smart Card Handbook. Fourth Edition. Wolfgang Rankl and Wolfgang Effing. Ed.- Wiley.2008.	Bibliografía	Bibliografía general
Smart Card Applications. Wolfgang Rankl. Ed. Wiley.2007.	Bibliografía	Bibliografía general
Plataforma moodle.	Recursos web	Plataforma para el desarrollo de la asignatura generada por el profesorado.
Software de libre distribución aplicable al contenido de la asignatura.	Equipamiento	Software para el desarrollo de aplicaciones prácticas
Aula equipada con ordenador, proyector de video, pizarra. Laboratorio con 10 ordenadores con software adecuado para la realización de las prácticas. Plataforma servidora PKI.	Equipamiento	

Tarjetas inteligentes, software y lectores de tarjetas para la realización de prácticas con éstas.	Otros	Material especifico para el desarrollo de la asignatura

9. Otra información

9.1. Otra información sobre la asignatura

Esta asignatura de Master se va a impartir en horario abreviado, por lo que la programación es susceptible de sufrir modificaciones para ajustar los contenidos presenciales al horario persencial real que se asigne a los alumnos.

Las competencias transversales se desarrollarán a través de los contenidos y prácticas a realizar en la asignatura.