BAB 4
IMPLEMENTASI DAN PENGUJIAN SISTEM

4.1 Implementasi

Tahap implementasi adalah tahap meletakan sistem agar siap untuk dioperasikan dan dapat dipandang sebagai usaha untuk mewujudkan sistem yang telah dirancang.

4.1.1 Lingkungan Implementasi

Pada lingkungan implementasi terdapat 2 lingkungan yang diimplementasi, yang pertama adalah implementasi keamanan sistem informasi dan yang kedua adalah implementasi *digital signature*.

4.1.2 Implementasi Keamanan Sistem Informasi

Implementasi keamanan sistem informasi pada sistem informasi pengusahaan air tanah ini direpresentasikan dengan kelas-kelas yang menerapkan keamanan sistem informasi pada sistem informasi pengusahaan air tanah

4.1.2.1 Implementasi Pembatasan Jumlah Percobaan Login

Berdasarkan hasil analisis dan perancangan keamanan sistem informasi pada poin pembatasan jumlah percobaan login, tahapan ini berdampak pada *method* login pada kelas *Auth.php*. Dalam *method* login sistem akan membaca data pada basis data untuk memeriksa jumlah percobaan login. Pada tabel 4.1 adalah kelas-kelas yang digunakan:

Tabel 4.1 Implementasi Kelas Autentikasi

Nama Kelas: Auth.php		
Jenis Method	**Nama Method**	**Deskripsi**
public	index()	Fungsi yang menampilkan halaman login
public	login()	Fungsi yang melakukan fungsionalitas login
public	logout()	Fungsi yang melakukan fungsionalitas logout
public	gagal_login()	Fungsi yang diakses jika terjadi kesalahan login
public	validation()	Fungsi yang diakses ketika validasi *username* dan *password*

4.1.2.2 Implementasi Penyaringan Data Masukan

Pada tahapan implementasi penyaringan data masukan secara *client side* yang terdampak bukanlah kelas, melainkan berkas yang secara langsung pengguna akses atau jika dalam paradigma MVC maka yang terdampak adalah bagian *view*. Ini dikarenakan penyaringan data masukan diterapkan pada sisi *client*, sehingga tidak diterapkan di kelas-kelas yang berhubungan.

Jika diterapkan pada kelas-kelas tertentu maka termasuknya penyaringan data masukan pada sisi *server*. Oleh karena itu, pada tabel 4.2 dijelaskan file-file *view* apa saja yang diimplementasikan penyaringan data masukan secara *client side*.

Tabel 4.2 Implementasi Penyaringan Data Masukan secara *client side*

Nama Antarmuka	Nama File	Deskripsi
Tambah data permohonan baru	v_tambah_baru.php	Digunakan untuk menambah data permohonan baru.
Tambah data permohonan perpanjangan	v_tambah_perpanjangan.php	Digunakan untuk menambah data permohonan perpanjangan.
Verifikasi data administrasi permohonan baru	v_verifikasi_baru.php	Digunakan untuk memverifikasi data administrasi permohonan baru.
Verifikasi data administrasi permohonan perpanjangan	v_verifikasi_perpanjangan.php	Digunakan untuk memverifikasi data administrasi permohonan perpanjangan.
Verifikasi data teknis permohonan baru	v_verifikasi_baru.php	Digunakan untuk memverifikasi data teknis permohonan baru
Verifikasi data teknis permohonan perpanjangan	v_verifikasi_perpanjangan.php	Digunakan untuk memverifikasi data teknis permohonan perpanjangan
Update data profil	v_tpl_profil.php	Digunakan untuk meng-update data profil

4.1.2.3 Implementasi Pencegahan Akses Langsung

Pada tahapan implementasi pencegahan akses langsung, hanya ada 2 *method* yang terdampak karena hanya 2 method tersebut adalah method yang menampilkan form untuk memasukan data verifikasi adminstrasi maupun teknis dan method yang menampilkan form untuk mengisi data-data pelengkap pembuatan *digital signature*. Pada tabel 4.3 dan 4.4 adalah implementasi pencegahan akses langsung.

Tabel 4.3 Implementasi Pencegahan Akses Langsung pada Method Verifikasi dan *Digital Signature*

Nama Kelas: Op_admin.php, Op_teknis.php, Pusat.php		
Jenis Method	**Nama Method**	**Deskripsi**
public	verifikasi()	Digunakan untuk memverifikasi permohonan surat baru atau perpanjangan
public	digsig()	Digunakan untuk menandatangani dokumen lembar kendali atau surat rekomendasi teknis.

Tabel 4.4 Implementasi Method *block_direct_access*

Nama Kelas: Rektek.php		
Jenis Method	**Nama Method**	**Deskripsi**
public	block_direct_access()	Digunakan untuk memeriksa URL acuan ketika mengakses halaman verifikasi dan *digital signature*.

4.1.3 Implementasi *Digital Signature*

Berikut ini adalah beberapa implementasi kegiatan yang dilakukan pada sistem informasi pengusahaan air tanah agar bisa menerapkan *digital signature*.

4.1.3.1 Implementasi Perubahan Basis Data

Implementasi pengubahan basis data dalam sistem informasi pengusahaan air tanah ini menggunakan perangkat lunak basis data MySQL. Berikut ini adalah sintaks *query* yang dieksekusi:

1. Tabel *t_digsig_baru*

   Tabel *t_digsig_baru* digunakan untuk menyimpan data *digital signature* untuk surat permohonan dengan jenis permohonan baru.

```
CREATE TABLE `t_digsig_baru` (
 `id_digsig` int(4) NOT NULL AUTO_INCREMENT,
 `id_user` int(2) DEFAULT NULL,
 `no_rektek_baru` int(6) DEFAULT NULL,
 `tgl_buat` datetime NOT NULL,
 `tgl_berlaku` date NOT NULL,
 `tgl_akhir` varchar(255) NOT NULL,
 `masa_berlaku` varchar(255) NOT NULL,
 `lokasi` varchar(25) NOT NULL,
 `alasan` varchar(101) NOT NULL,
 `path_private` varchar(201) DEFAULT NULL,
 `path_public` varchar(201) DEFAULT NULL,
 `jenis_dok` varchar(7) NOT NULL,
 PRIMARY KEY (`id_digsig`),
 KEY `fk_rektek_baru_sign` (`no_rektek_baru`),
 KEY `fk_user_baru_sign` (`id_user`),
 CONSTRAINT `fk_user_baru_sign` FOREIGN KEY (`id_user`)
REFERENCES `t_user` (`id_user`) ON DELETE SET NULL ON
UPDATE CASCADE
) ENGINE=InnoDB AUTO_INCREMENT=1 DEFAULT CHARSET=latin1;
```

2. Tabel *t_digsig_perpanjang*

   Tabel *t_digsig_perpanjang* digunakan untuk menyimpan data digital signature untuk surat permohonan dengan jenis permohonan perpanjangan.

```
CREATE TABLE `t_digsig_perpanjang` (
 `id_digsig` int(4) NOT NULL AUTO_INCREMENT,
 `id_user` int(2) DEFAULT NULL,
 `no_rektek_perpanjang` int(6) DEFAULT NULL,
 `tgl_buat` datetime NOT NULL,
 `tgl_berlaku` date NOT NULL,
 `tgl_akhir` varchar(255) NOT NULL,
 `masa_berlaku` varchar(255) NOT NULL,
 `lokasi` varchar(25) NOT NULL,
 `alasan` varchar(101) NOT NULL,
 `path_private` varchar(201) DEFAULT NULL,
 `path_public` varchar(201) DEFAULT NULL,
 `jenis_dok` varchar(7) NOT NULL,
 PRIMARY KEY (`id_digsig`),
 KEY `fk_user_sign` (`id_user`),
 KEY `fk_rektek_baru_sign` (`no_rektek_perpanjang`),
 CONSTRAINT `fk_rektek_perpanjang_sign` FOREIGN KEY
(`no_rektek_perpanjang`) REFERENCES `t_rektek_perpanjang`
(`no_rektek_perpanjang`) ON DELETE SET NULL ON UPDATE
CASCADE,
 CONSTRAINT `fk_user_perpanjang_sign` FOREIGN KEY
(`id_user`) REFERENCES `t_user` (`id_user`) ON DELETE SET
NULL ON UPDATE CASCADE
) ENGINE=InnoDB AUTO_INCREMENT=2 DEFAULT CHARSET=latin1;
```

3. Tabel *t_dname*

   Tabel *t_dname* digunakan untuk menyimpan data Pusat Sumber Daya Air Tanah dan Geologi Lingkungan selaku penyelenggara *digital signature*.

```
CREATE TABLE `t_dname` (
 `id` int(1) NOT NULL,
 `cn` varchar(2) NOT NULL,
 `sp` varchar(100) NOT NULL,
 `ln` varchar(100) NOT NULL,
 `o` varchar(100) NOT NULL,
 `ou` varchar(100) NOT NULL,
 `e` varchar(50) NOT NULL,
 PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=latin1;
```

4. Penambahan field pada tabel *t_user*.

   Field yang ditambahkan adalah alamat, id lokasi, tanggal lahir dan lokasi atau path gambar tanda tangan.

```
ALTER TABLE `t_user`
ADD COLUMN `alamat` varchar(201) NOT NULL,
ADD COLUMN `id_lokasi` int(5) DEFAULT NULL,
ADD COLUMN `kota_lahir` varchar(51) NOT NULL,
ADD COLUMN `tgl_lahir` date NOT NULL,
ADD COLUMN `sign_path` varchar(100) NOT NULL;
```

5. Penambahan field pada tabel *t_rektek_baru* dan *t_rektek_perpanjangan*.

   Field yang ditambahkan adalah signed_adm, signed_teknis, signed_si.

```
ALTER TABLE `t_rektek_baru`
ADD COLUMN `signed_adm` int(1) NOT NULL DEFAULT 0,
ADD COLUMN `signed_teknis` int(1) NOT NULL DEFAULT 0,
ADD COLUMN `signed_si` int(1) NOT NULL DEFAULT 0;
```

```
ALTER TABLE `t_rektek_perpanjang`
ADD COLUMN `signed_adm` int(1) NOT NULL DEFAULT 0,
ADD COLUMN `signed_teknis` int(1) NOT NULL DEFAULT 0,
ADD COLUMN `signed_si` int(1) NOT NULL DEFAULT 0;
```

4.1.3.2 Implementasi Pembuatan *Digital Signature*

Implementasi *digital signature* pada sistem informasi pengusahaan air tanah ini dimulai dengan pengguna mengunggah gambar tanda tangan. Pada tabel 4.5 dan 4.6 adalah kelas-kelas yang digunakan. Sedangkan implementasi pembuatan tanda tangan digital direpresentasikan dengan kelas-kelas yang mengelola data dan menerapkanya pada dokumen lembar kendali atau surat rekomendasi teknis. Pada tabel 4.7 adalah kelas yang digunakan.

Tabel 4.5 Implementasi Pengembangan Kelas untuk Pengunggahan Gambar Tanda Tangan

Nama Kelas: Op_admin.php, Op_teknis.php, Pusat.php		
Jenis Method	**Nama Method**	**Deskripsi**
public	profil()	Digunakan untuk menampilkan halaman unggah gambar tanda tangan
public	simpan()	Digunakan untuk memanggil fungsi upload_signature() pada kelas Rektek.php untuk mengunggah gambar tanda tangan

Tabel 4.6 Implementasi Pengembangan Kelas untuk Pengunggahan Gambar Tanda Tangan

Nama Kelas: Rektek.php		
Jenis Method	**Nama Method**	**Deskripsi**
public	upload_signature()	Method yang melakukan fungsionalitas unggah gambar

Tabel 4.7 Implementasi Kelas *Digital Signature*

Nama Kelas: Digital_signatures.php		
Jenis Method	**Nama Method**	**Deskripsi**
private	_set_dn()	Mengatur data *Distinguised Name*
private	_generate_keys()	Membangkitkan kunci public dan privat
public	key_data()	Mengambil alamat kunci publik dan privat
public	sign()	Menandatangani dokumen
public	start_sign_session()	Mengaktifkan sesi penandatanganan
public	check_sign_session()	Memeriksa sesi penandatanganan

4.1.3.3 Implementasi Antarmuka

Implementasi antarmuka pada sistem informasi pengusahaan air tanah ini meliputi antarmuka untuk pengunggahan gambar tanda tangan dan antarmuka penandatanganan dokumen lembar kendali atau surat rekomendasi teknis. Pada tabel 4.8 adalah penjelasan implementasi antarmuka.

Tabel 4.8 Implementasi Antarmuka

Nama Antarmuka	Nama File	Deskripsi
Pengunggahan gambar tanda tangan	v_tpl_profil.php	Digunakan untuk memudahkan pengguna mengunggah gambar tanda tangan
Digital Signature	v_tpl_digsig.php	Digunakan untuk mengumpulkan data-data yang diperlukan untuk membuat dan menerapkan *digital signature*

4.2 Pengujian Sistem

Pengujian sistem adalah tahapan sistem diuji sesuai dengan fungsionalnya. Terbagi menjadi 2 bagian yaitu rencana pengujian dan pengujian alpha.

4.2.1 Rencana Pengujian

Rencana pengujian yang akan dilakukan dengan menguji sistem secara alpha. Rencana pengujian penerapan keamanan sistem informasi dan digital signature pada sistem informasi pengusahaan air tanah adalah sebagai berikut

4.2.1.1 Rencana Pengujian Keamanan Sistem Informasi

Pada tabel 4.9 adalah rincian rencana pengujian keamanan sistem informasi

Tabel 4.9 Rencana Pengujian Keamanan Sistem Informasi

Jenis Uji	Butir Uji	Jenis Pengujian
Pembatasan jumlah percobaan login	Memasukan 6 kali data salah	Blackbox
Penyaringan data masukan secara *client side*	Memasukan karakter alfabet pada kolom numerik	Blackbox
	Memasukan *string* bukan dengan format email pada kolom email	Blackbox
	Memasukan karakter numeric sesuai format yang diminta	Blackbox
	Memasukan karakter numerik pada kolom nama	Blackbox
Pencegahan akses langsung	Mengakses halaman verifikasi secara langsung	Blackbox
	Mengakses halaman digital signature secara langsung	Blackbox

4.2.1.2 Rencana Pengujian *Digital Signature*

Pada tabel 4.10 adalah rincian rencana pengujian *digital signature.*

Tabel 4.10 Rencana Pengujian *Digital Signature*

Jenis Uji	Butir Uji	Jenis Pengujian
Digital Signature pada permohonan baru	Digital signature pada verifikasi administrasi	Blackbox
	Digital signature pada verifikasi teknis	Blackbox
	Digital signature pada surat rekomendasi teknis	Blackbox
Digital Signature pada permohonan perpanjangan	Digital signature pada verifikasi administrasi	Blackbox
	Digital signature pada verifikasi teknis	Blackbox
	Digital signature pada surat rekomendasi teknis	Blackbox

4.2.2 Pengujian Alpha

Hasil implementasi keamanan sistem informasi dan digital signature harus diuji terlebih dahulu agar sistem yang dibangun dapat berjalan dengan baik. Data masukan atau data yang akan diujikan ditentukan berdasarkan kebutuhan rencana pengujian. Berikut ini adalah tahapan pengujian alpha

4.2.2.1 Pengujian Alpha Keamanan Sistem Informasi

Pengujian yang dilakukan adalah menguji hasil implementasi keamanan sistem informasi yang diterapkan, diantarnya dijelaskan pada tabel 4.11 untuk data benar dan tabel 4.12 untuk data salah

Tabel 4.11 Pengujian Keamanan Sistem Informasi Data Benar

Data Masukan	Keluaran yang Diharapkan	Pengamatan	Kesimpulan
Data login benar Username: “admin” dan password: “admin123”	User admin masuk kedalam sistem	User admin masuk kedalam sistem	Diterima
Karakter numerik pada kolom numerik	Karakter numerik muncul pada kolom yang bersangkutan	Karakter numerik muncul pada kolom yang bersangkutan	Diterima
Karakter numeric pada halaman verifikasi teknis	Setiap karakter yang dimasukan mengikuti format yang sudah ditetapkan	Karakter selain numeric tidak muncul dan sesuai format	Diterima
String “Try Fathur Rachman” pada kolom nama	Karakter muncul pada kolom nama	Karakter muncul pada kolom nama	Diterima

Data Masukan	Keluaran yang Diharapkan	Pengamatan	Kesimpulan
Mengakses halaman verifikasi dari halaman acuan	Sistem menampilkan halaman verifikasi	Sistem menampilkan halaman verifikasi	Diterima
Mengakses halaman digital signature dari halaman acuan	Sistem menampilkan halaman digital signature	Sistem menampilkan halaman digital signature	Diterima

Tabel 4.12 Pengujian Keamanan Sistem Informasi Data Salah

Data Masukan	Keluaran yang Diharapkan	Pengamatan	Kesimpulan
Data login salah dan dicoba sebanyak 2 s/d 5 kali	Pesan kesalahan username atau password muncul	Pesan kesalahan username atau password muncul	Diterima
Data login salah dan dicoba sebanyak 6 kali atau lebih	Pesan kesalahan peringatan untuk tidak bisa login selama 15 muncul	User admin tidak bisa login selama 15 menit kedepan	Diterima
Karakter alphabet pada kolom numerik	Karakter alphabet tidak muncul pada kolom numerik	Karakter alphabet tidak muncul pada kolom numerik	Diterima
String dengan karakter “@” dan “.(domain)”	Pesan kesalahan tidak muncul pada kolom email	Pesan kesalahan tidak muncul pada kolom email	Diterima
String dengan karakter “@” dan string tanpa “.(domain)”	Pesan kesalahan muncul pada kolom email	Pesan kesalahan muncul pada kolom email	Diterima
String tanpa karakter “@” dan string tanpa “.(domain)”	Pesan kesalahan muncul pada kolom email	Pesan kesalahan muncul pada kolom email	Diterima
Karakter numeric “12345678987612345”pada kolom NIP	Pesan kesalahan “jumlah karakter kurang dari 18” muncul pada kolom NIP	Pesan kesalahan muncul pada kolom NIP	Diterima
Karakter numeric “1234567898761234522”pada kolom NIP	Karakter ke-19 tidak muncul pada kolom NIP	Karakter ke-19 tidak muncul pada kolom NIP	Diterima
String “Fatur 123” pada kolom nama	Karakter numerik tidak muncul pada kolom nama	Karakter numerik tidak muncul pada kolom nama	Diterima
Mengakses langsung halaman verifikasi	Ditolak dan menampilkan pesan kesalahan	Ditolak dan menampilkan pesan kesalahan	Diterima
Mengakses langsung halaman digital signature	Ditolak dan menampilkan pesan kesalahan	Ditolak dan menampilkan pesan kesalahan	Diterima

4.2.2.2 Pengujian Alpha Digital Signature

Pengujian yang dilakukan adalah menguji hasil implementasi digital signature yang diterapkan, diantarnya dijelaskan pada tabel 4.13 untuk pengujian data benar dan 4.14 untuk pengujian data salah

Tabel 4.13 Pengujian Digital Signature Data Benar

Data Masukan	Keluaran yang Diharapkan	Pengamatan	Kesimpulan
Data digital signature benar petugas administrasi Password: “12345678” Masa berlaku: 8 hari Kota: Bandung	Sistem membuat kunci public dan privat kemudian menyematkannya ke lembar kendali beserta gambar tanda tangan	Halaman berpindah dan memberikan pesan “Dokumen berhasil di tanda tangan”	Diterima
Data digital signature petugas teknis benar Password: “87654321” Masa berlaku: 8 hari Kota: Bandung	Sistem membuat kunci public dan privat kemudian menyematkannya ke lembar kendali beserta gambar tanda tangan	Halaman berpindah dan memberikan pesan “Dokumen berhasil di tanda tangan”	Diterima
Data digital signature Kepala Badan Geologi benar Password: “Geologi” Masa berlaku: 8 hari Kota: Bandung	Sistem membuat kunci public dan privat kemudian menyematkannya ke lembar kendali beserta gambar tanda tangan	Halaman berpindah dan memberikan pesan “Dokumen berhasil di tanda tangan”	Diterima

Tabel 4.14 Pengujian Digital Signature Data Salah

Data Masukan	Keluaran yang Diharapkan	Pengamatan	Kesimpulan
Data digital signature untuk petugas administrasi salah Password: “12345679” Masa berlaku: 8 hari Kota: Bandung	Kunci public dan privat gagal dibuat	Sistem menampilkan pesan “Password yang dimasukan salah”	Diterima
Data digital signature untuk petugas teknis salah Password: “12345678” Masa berlaku: 8 hari Kota: Bandung	Kunci public dan privat gagal dibuat	Sistem menampilkan pesan “Password yang dimasukan salah”	Diterima
Data digital signature untuk Kepala Badan Geologi salah Password: “Diponegoro” Masa berlaku: 8 hari Kota: Bandung	Kunci public dan privat gagal dibuat	Sistem menampilkan pesan “Password yang dimasukan salah”	Diterima

4.2.2.3 Kesimpulan Pengujian Alpha

Berdasarkan hasil pengujian alpha (fungsional) dengan kasus uji diatas dapat ditarik kesimpulan bahwa penerapan keamanan sistem informasi dan digital signature secara fungsional, sistem sudah dapat digunakan dan berjalan sesuai dengan yang diharapkan.